

Tunkeutumis- ja puolustusmenetelmät

Digital Forensics Henkilötyö

Mikael Romanov

Assignment
Maaliskuu 2018
Tieto- ja viestintätekniikka
Kyberturvallisuus

1 Table of Contents

| | | |
|----------|---|-----------|
| 1 | Johdanto | 3 |
| 2 | Työkalut | 4 |
| 2.1 | Autopsy 4.6.0 | 4 |
| 2.2 | Registry Explorer v1.0.0.0 | 4 |
| 2.3 | Kernel OST Viewer | 4 |
| 3 | Testausympäristö | 5 |
| 3.1 | Lenovo w520 | 5 |
| 3.2 | Levykuvat | 5 |
| 3.3 | Rekisterit | 6 |
| 4 | Järjestelmä | 8 |
| 4.1 | Levykuvien tiivistesummat | 8 |
| 4.2 | Käyttöjärjestelmän tiedot | 8 |
| 4.3 | Työaseman nimi | 10 |
| 4.4 | Viimeisin kirjautunut käyttäjä | 11 |
| 4.5 | Viimeisin työaseman sammutus | 11 |
| 4.6 | Verkkokorttien IP-osoite | 13 |
| 4.7 | Informantin asentamat ohjelmat | 14 |
| 5 | Verkkoselaimet ja Historia | 19 |
| 5.1 | Työaseman Web-selaimet | 19 |
| 5.2 | Hakemistot ja polut selaushistoriassa | 21 |
| 5.3 | Informantin vierailleet sivustot | 22 |
| 5.4 | Informantin käyttämät hakutermit | 25 |
| 6 | Verkkolevyt ja massamuistit | 27 |
| 6.1 | Liitetyt massamuistit | 27 |
| 6.2 | NAS IP-osoite | 29 |
| 6.3 | Verkkolevytä avatut tiedostot | 30 |
| 6.4 | Pilvipalveluihin liittyvät jäljet | 31 |

| | | |
|----------|---|-----------|
| 6.5 | Google Drivesta poistetut tiedostot | 33 |
| 6.6 | Herra Informantin irtisanoutuminen..... | 34 |
| 6.7 | Roskakori | 35 |
| 6.8 | Työasemalta kopioidut tiedostot massamuistille..... | 36 |
| 6.9 | Tiedostojen palautus USB massamuistilta | 39 |
| 7 | Anti-forensiikka..... | 41 |
| 7.1 | Muutettuja rekisteriavaimia 23-25.3.2015 | 41 |
| 7.2 | Forensiikka työtä vaikeuttavia toimenpiteitä..... | 42 |
| 7.3 | Oleellisia asioita tutkimuksessa | 43 |
| 7.4 | Todisteet tietovuodosta | 45 |
| 7.5 | Aikajana tapahtumista..... | 46 |
| 8 | Pohdinta | 47 |
| 9 | Lähteet..... | 47 |

1 Johdanto

Harjoituksen toimeksiantajana toimi Marko Vatanen, joka antoi tehtäväksi tutkia ja analysoida laman Informantin levykuvia. Herra Informantia syyllistettiin tietovuodosta, joten levykuvissa oli mahdollisia todisteita herra Informantin toteuttaneesta tietovuodosta. Toimeksiannosta tuli selville, että herra Informant pyrki tehokkaasti piiloittamaan todistuaaineiston ennen kiinni jäämistä. Vihjeiden mukaan hän oli käynyt keskusteluita sähköpostilla, jakanut pilvipalvelussa tietoa, sekä siirtänyt salaisia tiedostoja massamuistille. Toimeksi annossa määritettiin, että työn tulee ainakin sisältää seuraava asiat:

- Mitkä ovat levykuvien tiivistesummat?
- Selitä työasemaan asennetun käyttöjärjestelmän tiedot (käyttöjärjestelmän nimi, asennuspäivä, rekisteröity omistaja...)
- Mikä on työaseman nimi?
- Kuka oli viimeisin työasemaan kirjautunut käyttäjä?
- Koska työasema on viimeisimmäksi sammutettu(päivä/aika)?
- Selitä verkkokorttien IP-osoite tiedot?
- Mitkä ohjelmat oli herra Informantin toimesta asennettu käyttöjärjestelmän asennuksen jälkeen?
- Mitä web-selaimia on käytettytyöasemassa?
- Selvitä mitä hakemistot/polut liittyvät selaushistoriaan
- Millä web-sivuilla herra Informant vieraili? (aikaleima ja URL)
- Listaa kaikki hakutermit joita käytetty web-selaimessa (aikaleima, URL, hakutermi
- Listaa ulkoiset massamuistit, jotka on työasemaan liitetty
- Mikä on yrityksen verkkolevy-palvelimen IP-osoite?
- Listaakaikki tiedostot, jotka avattiin verkkolevyltä
- Etsi kaikki jäljet, jotka liittyvät pilvipalveluihin
- Mitkä tiedostot on poistettu Google Drivestä?
- Koska herra Informant tulosti irtosanoutumispaperin?
- Tutki Windowsin roskakori
- Mitä tiedostoja on työasemaltakopioitu USB-muistilla (levykuva RM#2)
- Palauta USB-muistilta poistetut tiedostot (levykuva RM#2)
- Mitä eri rekisteriavaimia on muutettu 23-25.3.2015 välisenä aikana?
- Minkälaisia toimenpiteitä on tehty vaikeuttamaan forensiikkatyötä 25.3.2015?
- Mitä muuta oleellista tutkimuksessa löysit?
- Saitko tarpeeksi todisteita tietovuodosta?
- Rakenna aikajana tapahtumista

(Marko Vatanen Digital Forensics -harjoitus 16.01.2017)

2 Työkalut

2.1 Autopsy 4.6.0

Työnä oli tutkia laman Informantin tietokoneesta otettuja offline levykuvia. Autopsy on ilmainen digitaalinen forensiikka työkalu graafisella käyttöliittymällä, joka on tarkoitettu levykuvien tutkimiseen. Autopsyä käyttää sekä lainvalvonta, yritysasiantuntijat, että yksityiset henkilöt. Autopsyä voi esimerkiksi käyttää pelkkien poistettujen tiedostojen palauttamiseen muistikortilta tai kovalevyltä. Autopsy toimii Linuxilla, ja tulee esimerkiksi KNOPPIX-distron mukana valmiiksi, Autopsy toimii myös Windowsilla sekä OSX:llä. Autopsyssä on seuraavanlaisia moduuleita:

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
- Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using STIX.

(Brian Carrier, Autopsy n.d.)

2.2 Registry Explorer v1.0.0.0

Registry Explorer on Eric R. Zimmermanin tekemä ilmainen työkalu, millä voi tarkastella ja analysoida offline levykuvasta exportattuja rekistereitä. Tehtävässä käytettiin Registry Exploreria tiettyjen rekistereiden tarkastelemiseen. (Eric Zimmerman Github, n.d.)

2.3 Kernel OST Viewer

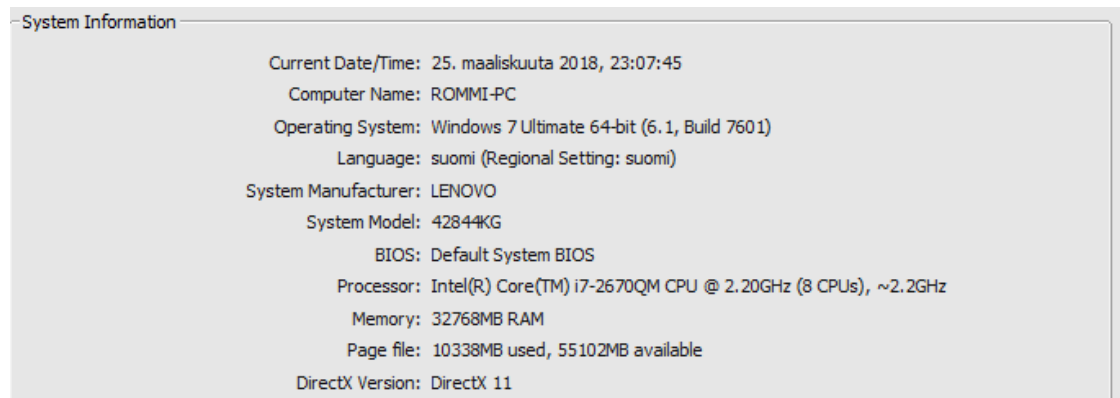
Kernel OST Viewer on ilmainen OST tiedostotyyppien tarkastelija. Kernel OST Viewerillä voi tarkastella MS Outlookin tiedostoja ilman MS Outlookia. Työkalulla voi nähdä kyseisen sähköpostikäyttäjän kaikki poistetut keskustelut, muistiinpanot,

käydyt keskustelut, jne. Työkalua käytettiin tehtävässä kun epäilyn Herra Informantin .ost tiedosto löytyi. (Kernel Data Recovery Kernel OST Viewer, n.d.)

3 Testausympäristö

3.1 Lenovo w520

Tehtävässä käytettiin Lenovo w520 kannettavaa tietokonetta analysoimaan levyosioita, sillä analysointi työkalut söivät huomattavan paljon resursseja ja työn suorittaminen oli helpompaa, kun prosessori tai muisti ei ollut pullonkaulana. (Kuvio 1)



Kuvio 1 Resurssit

3.2 Levykuvat

Itse testattavan ympäristön sai ladattua koulun verkkolevyjaolta:

<\\ghost.labranet.jamk.fi\\virtuaalikoneet\\TTKS1000>. Levykuvia oli yhteensä 6

kappaletta (1PC 4 osiointia ja 2kpl massamuistilaitteita) kooltaan 7.61GB. Levykuvat paisuivat analyyst projektin luomisessa ~10 gigaa lisää, jolloin projektin koko oli noin 20GB. Levykuvien formaatit sisältävät Windows käyttöjärjestelmän, levykuvat olivat NTFS tyyppiä, vol2 koko oli 100MB ja vol3 oli 19.9GB (Kuvio 2)

| /img_2015_data_leakage_pc.E01 | | | | | |
|---|----|-----------------|-------------------|---------------------|-------------|
| Table Thumbnail | | | | | |
| Name | ID | Starting Sector | Length in Sectors | Description | Flags |
| vol1 (Unallocated: 0-2047) | 1 | 0 | 2048 | Unallocated | Unallocated |
| vol2 (NTFS / exFAT (0x07): 2048-206847) | 2 | 2048 | 204800 | NTFS / exFAT (0x07) | Allocated |
| vol3 (NTFS / exFAT (0x07): 206848-41940991) | 3 | 206848 | 41734144 | NTFS / exFAT (0x07) | Allocated |
| vol4 (Unallocated: 41940992-41943039) | 4 | 41940992 | 2048 | Unallocated | Unallocated |

Kuvio 2 Levyosiot

Irroitettava massamuistin vol2 oli tiedosto tyyppiä FAT32 ja kooltaan

| /img_2015_data_leakage_rm#2.E01 | | | | | |
|--|----|-----------------|-------------------|--------------------|-------------|
| Table Thumbnail | | | | | |
| Name | ID | Starting Sector | Length in Sectors | Description | Flags |
| vol1 (Unallocated: 0-127) | 1 | 0 | 128 | Unallocated | Unallocated |
| vol2 (Win95 FAT32 (0x0b): 128-2097279) | 2 | 128 | 2097152 | Win95 FAT32 (0x0b) | Allocated |
| vol3 (Unallocated: 2097280-7821311) | 3 | 2097280 | 5724032 | Unallocated | Unallocated |

Kuvio 3 massamuisti osiot

3.3 Rekisterit

Analysointia varten levykuvista tarvitsi exportata rekisterit, joita tehtävässä käytettiin. Käytetyt rekisterit löytyivät vol3 osiosta Windows/system32/config/ hakemista alta. (Kuvio 4) Valitut rekisterit menivät mututuntumalta, sillä jokainen niistä sisälsi erilaista dataa, vasta kysymyksiä suorittaessa tuli selville oikeasti tarvittavat rekisterit. (Kuvio 5)

| Name | Modified Time | Change Time | Access Time | Created Time |
|--|--------------------------|-------------------------|--------------------------|--------------------------|
| COMPONENTS(016888b9-6c6f-11de-8d1d-001e0bde3ec).TM.bif | 2015-03-25 17:00:52 EET | 2015-03-25 17:00:52 EET | 2009-07-14 07:54:56 EEST | 2009-07-14 07:54:56 EEST |
| COMPONENTS(016888b9-6c6f-11de-8d1d-001e0bde3ec).TMCon | 2015-03-25 17:00:52 EET | 2015-03-25 17:00:52 EET | 2009-07-14 07:54:56 EEST | 2009-07-14 07:54:56 EEST |
| COMPONENTS(016888b9-6c6f-11de-8d1d-001e0bde3ec).TMCon | 2009-07-14 08:01:27 EEST | 2015-03-25 13:09:29 EET | 2009-07-14 07:54:56 EEST | 2009-07-14 07:54:56 EEST |
| DEFAULT | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST |
| DEFAULT.LOG | 2010-11-21 09:20:59 EET | 2015-03-25 13:13:48 EET | 2010-11-21 09:20:59 EET | 2009-07-14 10:07:31 EEST |
| DEFAULT.LOG1 | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| DEFAULT.LOG2 | 2009-07-14 05:34:08 EEST | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SAM | 2015-03-25 17:31:05 EET | 2015-03-25 16:46:37 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST |
| SAM.LOG | 2010-11-21 09:20:59 EET | 2015-03-25 13:13:48 EET | 2010-11-21 09:20:59 EET | 2009-07-14 10:07:31 EEST |
| SAM.LOG1 | 2015-03-25 16:46:37 EET | 2015-03-25 16:46:37 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SAM.LOG2 | 2009-07-14 05:34:08 EEST | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SECURITY | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST |
| SECURITY.LOG | 2010-11-21 09:20:59 EET | 2015-03-25 13:13:48 EET | 2010-11-21 09:20:59 EET | 2009-07-14 10:07:30 EEST |
| SECURITY.LOG1 | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SECURITY.LOG2 | 2009-07-14 05:34:08 EEST | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SOFTWARE | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST |
| SOFTWARE.LOG | 2010-11-21 09:21:00 EET | 2015-03-25 13:13:50 EET | 2010-11-21 09:21:00 EET | 2009-07-14 10:07:30 EEST |
| SOFTWARE.LOG1 | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SOFTWARE.LOG2 | 2009-07-14 05:34:08 EEST | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SYSTEM | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST |
| SYSTEM.LOG | 2010-11-21 09:20:59 EET | 2015-03-25 13:13:50 EET | 2010-11-21 09:20:59 EET | 2009-07-14 10:07:30 EEST |
| SYSTEM.LOG1 | 2015-03-25 17:31:05 EET | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| SYSTEM.LOG2 | 2009-07-14 05:34:08 EEST | 2015-03-25 17:31:05 EET | 2009-07-14 05:34:08 EEST | 2009-07-14 05:34:08 EEST |
| COMPONENTS | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| COMPONENTS | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |

Kuvio 4 Rekisterit 1

| Registry hive | Supporting files |
|------------------------------------|--|
| HKEY_CURRENT_CONFIG | System, System.alt, System.log, System.sav |
| HKEY_CURRENT_USER | Ntuser.dat, Ntuser.dat.log |
| HKEY_LOCAL_MACHINE\SAM | Sam, Sam.log, Sam.sav |
| HKEY_LOCAL_MACHINE\Security | Security, Security.log, Security.sav |
| HKEY_LOCAL_MACHINE\Software | Software, Software.log, Software.sav |
| HKEY_LOCAL_MACHINE\System | System, System.alt, System.log, System.sav |
| HKEY_USERS\DEFAULT | Default, Default.log, Default.sav |

Kuvio 5 Microsoft Registry Hives ([https://msdn.microsoft.com/en-us/library/windows/desktop/ms724877\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms724877(v=vs.85).aspx))

Käyttäjä kohtainen rekisteri ntuser.dat löytyi /Users/Informant/ alta (Kuvio 6)

/img_2015_data_leakage_pc.E01/vol_vol3/Users/Informant

| Name | Modified Time | Change Time | Access Time | Created Time | Size |
|-------------------------------|-------------------------|-------------------------|-------------------------|-------------------------|---------|
| Local Settings | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Music | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:41 EET | 152 |
| My Documents | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| NetHood | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Pictures | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:41 EET | 152 |
| PrintHood | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Recent | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Saved Games | 2015-03-24 20:29:10 EET | 2015-03-24 20:29:10 EET | 2015-03-24 20:29:10 EET | 2015-03-22 16:34:41 EET | 368 |
| Searches | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-22 16:34:55 EET | 56 |
| SendTo | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Start Menu | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Templates | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Videos | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:41 EET | 152 |
| NTUSER.DAT | 2015-03-22 16:34:59 EET | 2015-03-25 17:30:57 EET | 2015-03-25 17:30:58 EET | 2015-03-22 16:34:41 EET | 1048576 |
| ntuser.dat.LOG1 | 2015-03-22 16:34:59 EET | 2015-03-25 17:30:57 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 262144 |
| ntuser.dat.LOG2 | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 0 |
| NTUSER.DAT{016888bd-6c6f-1... | 2015-03-22 16:38:15 EET | 2015-03-22 16:38:15 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 65536 |
| NTUSER.DAT{016888bd-6c6f-1... | 2015-03-22 16:38:15 EET | 2015-03-22 16:38:15 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 524288 |
| NTUSER.DAT{016888bd-6c6f-1... | 2015-03-22 16:38:15 EET | 2015-03-22 16:38:15 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 524288 |
| ntuser.ini | 2015-03-25 15:06:09 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 20 |

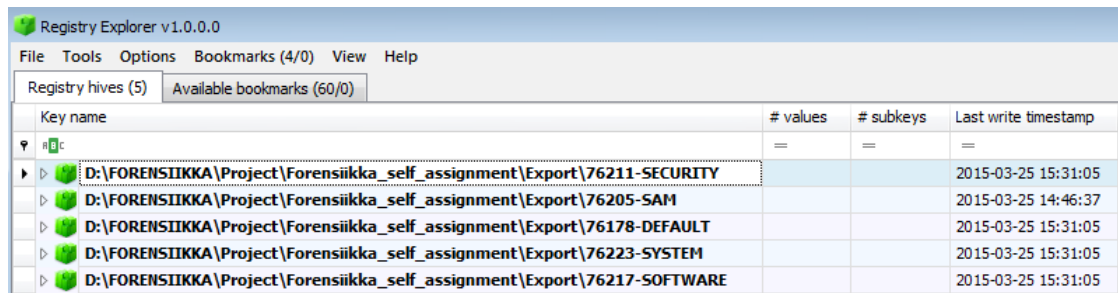
Properties
View in New Window
Open in External Viewer
View File in Timeline...
Extract File(s)
Search for files with the same MD5 hash
Tag File
Remove File Tag
Add file to hash database

Hex Strings File Metadata Results

Matches on page: - of -

Kuvio 6 Rekisterit 2

Exporttauksen jälkeen rekisterit pystyi tuoda Registry Explorer ohjelmaan, josta pystyi tutkia rekistereiden sisältöjä (Kuvio 7)



Kuvio 7 Import rekisteri

4 Järjestelmä

4.1 Levykuvien tiivistesummat

Levykuvien MD5-tiivistesummat sai selville valitsemalla Data Sources valinnan (Kuvio 8)

| Name | Type | Size (Bytes) | Sector Size (Bytes) | MD5 Hash | Timezone | Device ID |
|----------------------------|-------|--------------|---------------------|----------------------------------|-----------------|--------------------------------------|
| 2015_data_leakage_pc.E01 | Image | 21474836480 | 512 | a49d1254c873808c58e6f1bcd60b5bde | Europe/Helsinki | 42b72eaf-21d2-4fd3-9c90-fa8ff778e652 |
| 2015_data_leakage_rm#2.E01 | Image | 4004511744 | 512 | b4644902acab4583a1d0f9f1a08faa77 | Europe/Helsinki | c91d262b-1e28-4056-b007-f5d39c379139 |

Kuvio 8 Tiivistesummat

PC MD5-HASH = A49D1254C873808C58E6F1BCD60B5BDE

RM#2 MD5-HASH = B4644902ACAB4583A1D0F9F1A08FAA77

4.2 Käyttöjärjestelmän tiedot

2.Selitä työasemaan asennetun käyttöjärjestelmän tiedot (käyttöjärjestelmän nimi, asennuspäivä, rekisteröity omistaja...)

Käyttöjärjestelmän tiedot asennuspäivästä, nimestä, versiosta, jne... löytyi SOFTWARE rekisterinalta polusta Microsoft/CurrentVersion. (Kuvio 9) Kuvasta voidaan päätellä seuraavia asioita:

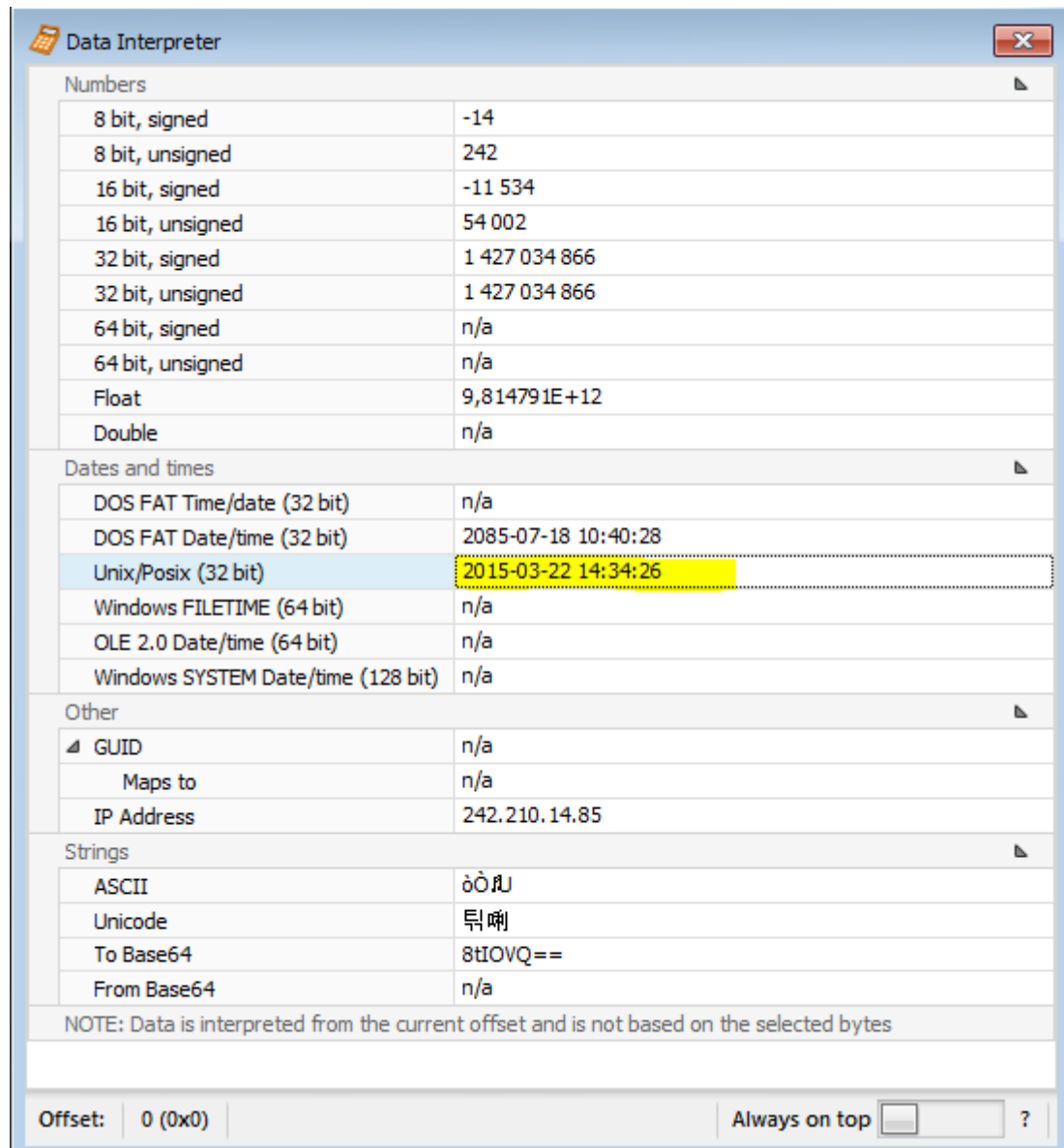
- Käyttöjärjestelmä: Windows 7 Ultimate (64 bit)
- Versio: 6.1
- Build nro: 7601
- Järjestelmän ROOT: C:\\Windows
- Rekisteröity käyttäjä: informant

| | Value Name | Value Type | Data | Value Slack |
|----------------|------------------------|------------|---|-------------------------------------|
| CurrentVersion | CurrentVersion | RegSz | 6.1 | 38-8C-44-00 |
| | CurrentBuild | RegSz | 7601 | 00-00 |
| | SoftwareType | RegSz | System | 00-00-00-00-00-00 |
| | CurrentType | RegSz | Multiprocessor Free | 65-00-64-00-00-00-6E-00-64-00-69-00 |
| | InstallDate | RegDword | 1427034866 | |
| | RegisteredOrganization | RegSz | | |
| | RegisteredOwner | RegSz | informant | 65-00-72-00-00-00-6C-00 |
| | SystemRoot | RegSz | C:\Windows | 00-00-00-00-00-00 |
| | InstallationType | RegSz | Client | 00-00-00-00-00-00 |
| | EditionID | RegSz | Ultimate | 00-00 |
| | ProductName | RegSz | Windows 7 Ultimate | 00-00-00-00-00-00 |
| | ProductId | RegSz | 00426-292-0000007-85262 | 69-63-72-6F |
| | DigitalProductId | RegBinary | A4-00-00-00-03-00-00-00-30-30-34-32-36-2D-32-39-32-2D-30-30-30-30-30-3... | |
| | DigitalProductId4 | RegBinary | F8-04-00-00-04-00-00-00-30-00-30-00-34-00-32-00-36-00-2D-00-30-00-30-0... | 00-00-00-00 |
| | CurrentBuildNumber | RegSz | 7601 | 00-00 |
| | BuildLab | RegSz | 7601.win7sp1_gdr.130828-1532 | 00-00 |
| | BuildLabEx | RegSz | 7601.18247.amd64fre.win7sp1_gdr.130828-1532 | 0C-00-00-00 |
| | BuildGUID | RegSz | cefa1a179-8b62-4cee-a99f-1c96c94a8e4d | 00-00 |
| | CSDBuildNumber | RegSz | 1130 | 00-00 |
| | PathName | RegSz | C:\Windows | 00-00-00-00-00-00 |
| | CSDVersion | RegSz | Service Pack 1 | 39-00-30-00-37-00 |

Kuvio 9 käyttöjärjestelmän tiedot

Tarkka asennus aika saatiin, kun InstallDatea tarkasteli Data Interpreterillä. (Kuvio 10)

Tarkka aika asennukselle oli 22.03.2015 klo 14.34:26 GMT



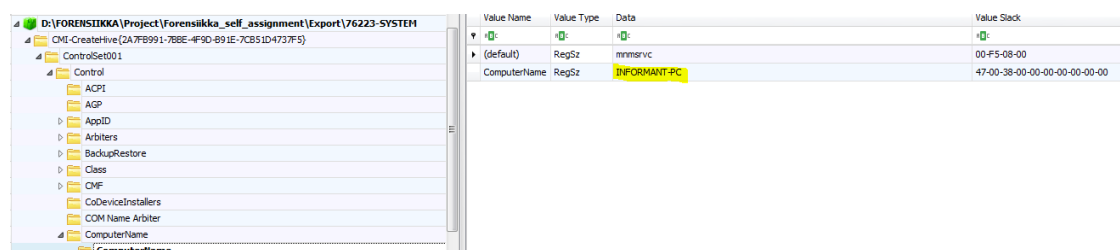
Kuvio 10 asennus aika

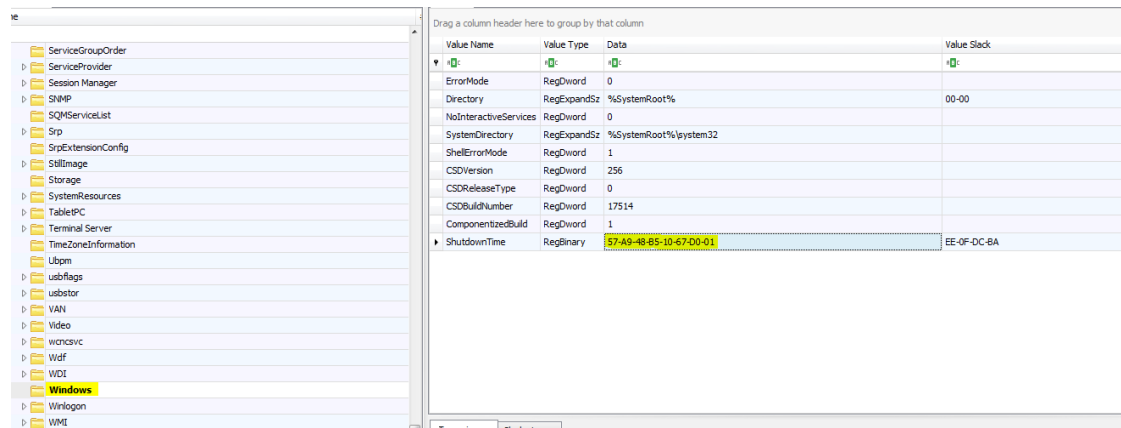
4.3 Työaseman nimi

Työaseman nimi löytyi SYSTEM rekisteri hiven alta hakemistosta

ControlSet001/Control/ComputerName/ (Kuvio 11). Tietokoneen nimi oli

INFORMANT-PC



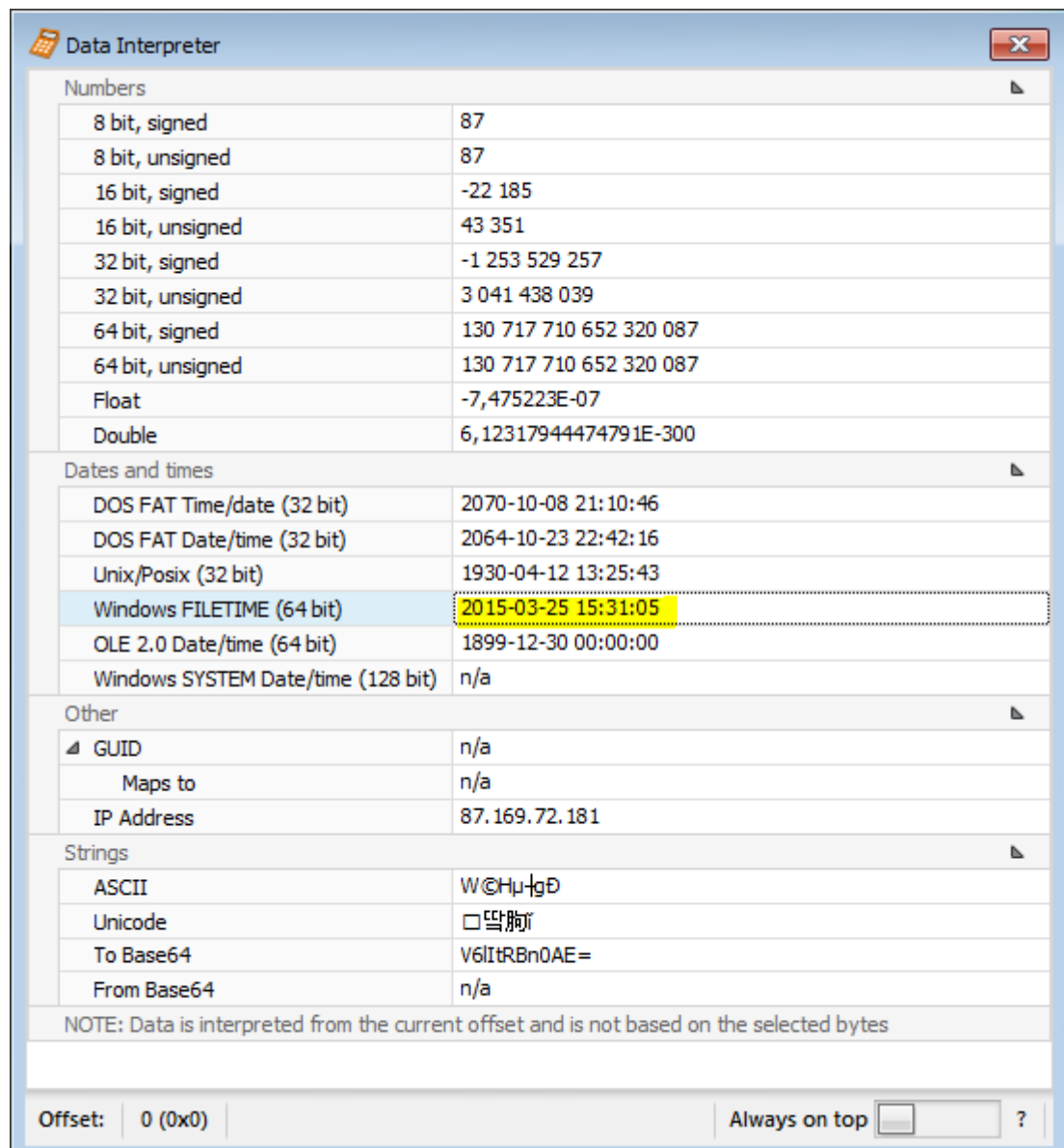


The screenshot shows the Windows Registry editor. The left pane displays the tree structure, with 'ShutdownTime' selected under 'System\CurrentControlSet\Control'. The right pane shows the details for this value.

| Value Name | Value Type | Data | Value Slack |
|--------------|------------|-------------------------|-------------|
| ShutdownTime | RegBinary | 57-A9-48-85-10-67-00-01 | EE-0F-DC-BA |

Kuvio 13 Viimeinen sammutus

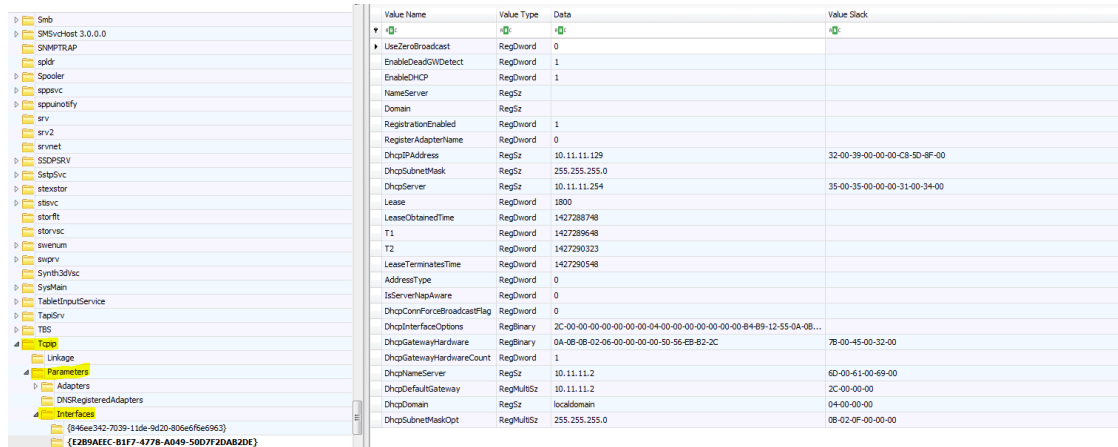
Kuvion 13 sammutus aika hexa arvoina ei kertonut mitään, joten Data Interpreterin avulla tiedosta sai paljon enemmän selvää. (Kuvio 14) Tarkka sammuttamisaika oli 25.03.2015 15.31:05 GMT



Kuvio 14 Sammutuksen tarkka aika

4.6 Verkkokorttien IP-osoite

Verkkokorttien IP-osoitteet pystyi löytämään SYSTEM hive rekisterin alta, joko ControlSet001 tai ControlSet002 alta. Kuvio 15 esimerkissä on käytetty ControlSet002/services/Tcpip/Parameters/Interfaces/



Kuvio 15 IP-osoite

| | |
|-----------------|--------------|
| IP-Osoite | 10.11.11.129 |
| DHCP-Serveri | 10.11.11.2 |
| Default Gateway | 10.11.11.2 |
| Dhcp Domain | localDomain |
| Maski | /24 |

4.7 Informantin asentamat ohjelmat

Herra Informantin asentamia ohjelmia löytyi useammasta paikkaa. Asennetut ohjelmat löytyivät nimensä mukaan SOFTWARE hive rekisterin alta Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall tai Microsoft/Windows/CurrentVersion/Uninstall. Herra Informant oli asentanut lukuisan ohjelman, joten seuraavien kuvioiden jälkeen löytyy taulukko ohjelmista, jotka Informant asensi. Kuvio 16, Kuvio 17, Kuvio 18, Kuvio 19 ja Kuvio 20 löytyivät Wow6432Noden alta.

Drag a column header here to group by that column

| Value Name | Value Type | Data | Value Slack |
|-----------------|------------|--|-------------------|
| ▼ | | | |
| ► DisplayName | RegSz | Google Chrome | |
| UninstallString | RegSz | "C:\Program Files (x86)\Google\Chrome\Application\41.0.2272.101\Installer\setup.exe" --uninstall --multi-install --chrome --system-level --verbose-logging | 00-00-00-00-00-00 |
| InstallLocation | RegSz | C:\Program Files (x86)\Google\Chrome\Application | 00-00 |
| DisplayIcon | RegSz | C:\Program Files (x86)\Google\Chrome\Application\chrome.exe,0 | |
| NoModify | RegDword | 1 | |
| NoRepair | RegDword | 1 | |
| Publisher | RegSz | Google Inc. | D3-65-A7-C2 |
| Version | RegSz | 41.0.2272.101 | |
| DisplayVersion | RegSz | 41.0.2272.101 | |
| InstallDate | RegSz | 20150322 | A1-02 |
| VersionMajor | RegDword | 2272 | |
| VersionMinor | RegDword | 101 | |

Kuvio 16 Chrome

| Value Name | Value Type | Data | Value Slack |
|---------------------|-------------|--|-------------------|
| ▼ | | | |
| AuthorizedCDFPrefix | RegSz | | |
| Comments | RegSz | | |
| Contact | RegSz | | |
| DisplayVersion | RegSz | 1.3.26.9 | B2-02 |
| HelpLink | RegSz | | |
| HelpTelephone | RegSz | | |
| InstallDate | RegSz | 20150322 | B2-02 |
| InstallLocation | RegSz | | |
| InstallSource | RegSz | C:\Program Files (x86)\Google\Update\1.3.26.9\ | 00-00-00-00-00-00 |
| ► ModifyPath | RegExpandSz | MsiExec.exe /I{60EC980A-8DA2-4CB6-A427-B07A5498B4CA} | 00-00 |
| Publisher | RegSz | Google Inc. | D8-FF-B2-02 |
| Readme | RegSz | | |
| Size | RegSz | | |
| EstimatedSize | RegDword | 29 | |
| SystemComponent | RegDword | 1 | |
| UninstallString | RegExpandSz | MsiExec.exe /I{60EC980A-8DA2-4CB6-A427-B07A5498B4CA} | 00-00 |
| URLInfoAbout | RegSz | | |
| URLUpdateInfo | RegSz | | |
| VersionMajor | RegDword | 1 | |
| VersionMinor | RegDword | 3 | |
| WindowsInstaller | RegDword | 1 | |
| Version | RegDword | 16973850 | |
| Language | RegDword | 1033 | |
| DisplayName | RegSz | Google Update Helper | 00-00 |

Kuvio 17 Google Update Helper

| Value Name | Value Type | Data | Value Slack |
|-----------------------|-------------|--|-------------------|
| ▼ | | | |
| ► AuthorizedCDFPrefix | RegSz | | |
| Comments | RegSz | | |
| Contact | RegSz | | |
| DisplayVersion | RegSz | 1.20.8672.3137 | 01-00-00-00-02-00 |
| HelpLink | RegExpandSz | http://www.google.com | |
| HelpTelephone | RegSz | http://www.google.com | |
| InstallDate | RegSz | 20150323 | CA-02 |
| InstallLocation | RegSz | | |
| InstallSource | RegSz | C:\Program Files (x86)\Google\Update\Install\{FADF88BF-D689-448E-BC51-AFD81CF380D1}\ | 00-63 |
| ModifyPath | RegExpandSz | MsiExec.exe /X{6C36881B-0E51-4231-9D02-BF2149664D34} | 00-33 |
| NoModify | RegDword | 1 | |
| NoRepair | RegDword | 1 | |
| Publisher | RegSz | Google, Inc. | 00-6F |
| Readme | RegSz | | |
| Size | RegSz | | |
| EstimatedSize | RegDword | 38784 | |
| UninstallString | RegExpandSz | MsiExec.exe /X{6C36881B-0E51-4231-9D02-BF2149664D34} | 00-79 |
| URLInfoAbout | RegSz | http://www.google.com | |
| URLUpdateInfo | RegSz | http://www.google.com | |
| VersionMajor | RegDword | 1 | |
| VersionMinor | RegDword | 20 | |
| WindowsInstaller | RegDword | 1 | |
| Version | RegDword | 18096608 | |
| Language | RegDword | 1033 | |
| DisplayName | RegSz | Google Drive | CA-02 |

Kuvio 18 Google Drive

| Value Name | Value Type | Data | Value Slack |
|---------------------|-------------|--|-------------------|
| AuthorizedCDFPrefix | RegSz | | |
| Comments | RegSz | | |
| Contact | RegSz | AppleCare Support | |
| DisplayVersion | RegSz | 3.0.6 | |
| HelpLink | RegExpandSz | http://www.apple.com/support/ | |
| HelpTelephone | RegSz | 1-800-275-2273 | 4C-50-00-00-00-00 |
| InstallDate | RegSz | 20150323 | 00-00 |
| InstallLocation | RegSz | C:\Program Files (x86)\Common Files\Apple\Apple Application Support\ | 00-38 |
| InstallSource | RegSz | C:\Users\INFORM~1\AppData\Local\Temp\IXP374.TMP\ | 00-00 |
| ModifyPath | RegExpandSz | MsExec.exe /I{78002155-F025-4070-85B3-7C0453561701} | 00-33 |
| Publisher | RegSz | Apple Inc. | AC-02-A8-8C-AC-02 |
| Readme | RegSz | | |
| Size | RegSz | | |
| EstimatedSize | RegDword | 96831 | |
| UninstallString | RegExpandSz | MsExec.exe /I{78002155-F025-4070-85B3-7C0453561701} | 00-00 |
| URLInfoAbout | RegSz | http://www.apple.com | 00-00 |
| URLUpdateInfo | RegSz | http://www.apple.com/ | |
| VersionMajor | RegDword | 3 | |
| VersionMinor | RegDword | 0 | |
| WindowsInstaller | RegDword | 1 | |
| Version | RegDword | 50331654 | |
| Language | RegDword | 1033 | |
| DisplayName | RegSz | Apple Application Support | |

Kuvio 19 Apple Application Support

| Value Name | Value Type | Data | Value Slack |
|---------------------|-------------|---|-------------------|
| AuthorizedCDFPrefix | RegSz | | |
| Comments | RegSz | | |
| Contact | RegSz | AppleCare Support | |
| DisplayVersion | RegSz | 2.1.3.127 | |
| HelpLink | RegExpandSz | http://www.apple.com/support/ | |
| HelpTelephone | RegSz | 1-800-275-2273 | 0B-C4-F0-B2-68-08 |
| InstallDate | RegSz | 20150323 | 00-2C |
| InstallLocation | RegSz | C:\Program Files (x86)\Apple Software Update\ | |
| InstallSource | RegSz | C:\Users\INFORM~1\AppData\Local\Temp\IXP374.TMP\ | 00-76 |
| ModifyPath | RegExpandSz | MsExec.exe /I{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE} | 00-00 |
| Publisher | RegSz | Apple Inc. | D2-02-D8-12-D2-02 |
| Readme | RegSz | | |
| Size | RegSz | | |
| EstimatedSize | RegDword | 2441 | |
| UninstallString | RegExpandSz | MsExec.exe /I{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE} | 00-00 |
| URLInfoAbout | RegSz | http://www.apple.com | 00-00 |
| URLUpdateInfo | RegSz | http://www.apple.com/ | |
| VersionMajor | RegDword | 2 | |
| VersionMinor | RegDword | 1 | |
| WindowsInstaller | RegDword | 1 | |
| Version | RegDword | 33619971 | |
| Language | RegDword | 1033 | |
| DisplayName | RegSz | Apple Software Update | |

Kuvio 20 Apple Software Update

Kuviot 21-24 ovat Microsoft/ hakemiston alta.

| Value Name | Value Type | Data | Value Slack |
|--------------------------|------------|---|-------------------|
| ▼ | ▼ | ▼ | ▼ |
| ► Publisher | RegSz | Microsoft Corporation | |
| CacheLocation | RegSz | C:\MSOCache\All Users | |
| DisplayIcon | RegSz | C:\Program Files\Common Files\Microsoft Shared\OFFICE15\Office Setup Controller\OSETUP.DLL, 1 | 00-00 |
| DisplayName | RegSz | Microsoft Office Professional Plus 2013 | 00-00-00-00 |
| DisplayVersion | RegSz | 15.0.4420.1017 | 00-00-00-00-00-00 |
| InstallLocation | RegSz | C:\Program Files\Microsoft Office | |
| ModifyPath | RegSz | "C:\Program Files\Common Files\Microsoft Shared\OFFICE15\Office Setup Controller\setup.exe" /modify PROPLUSR /dll OSETUP.DLL | 00-00 |
| NoElevateOnModify | RegDword | 0 | |
| NoModify | RegDword | 0 | |
| NoRemove | RegDword | 0 | |
| NoRepair | RegDword | 1 | |
| PackageRefs | RegMultiSz | AccessMUISet.en-us OfficeMUI.en-us ExcelMUI.en-us OfficeMUISet.en-us InfoPathMUI.en-us Office32MUI.en-us AccessMUI.en-us PowerPointMUI... | 00-00 |
| ProductCodes | RegMultiSz | {90150000-006E-0409-1000-0000000FF1CE} {90150000-001B-0409-1000-0000000FF1CE} {90150000-001A-0409-1000-0000000FF1CE} {901500... | |
| ShellUITransformLanguage | RegSz | en-US | |
| SkuComponents | RegMultiSz | C:\Program Files\Common Files\Microsoft Shared\OFFICE15\Office Setup Controller\DCF.en-us\setup.xml C:\Program Files\Common Files\Microsoft ... | 00-00-00-00-00-00 |
| SPPSkuld | RegMultiSz | 1B686580-9FB1-4B88-BFBA-EAE7C0DA31AD | |
| UninstallString | RegSz | "C:\Program Files\Common Files\Microsoft Shared\OFFICE15\Office Setup Controller\setup.exe" /uninstall PROPLUSR /dll OSETUP.DLL | 00-00-00-00 |
| VersionMajor | RegDword | 15 | |
| VersionMinor | RegDword | 0 | |
| ProductID | RegSz | 00216-00000-00000-AA352 | 00-00-00-00 |

Kuvio 21 Microsoft Office Professional Plus 2013

| Value Name | Value Type | Data | Value Slack |
|-----------------------|-------------|--|-------------------|
| ▼ | ▼ | ▼ | ▼ |
| ► AuthorizedCDFPrefix | RegSz | | |
| Comments | RegSz | | |
| Contact | RegSz | AppleCare Support | |
| DisplayVersion | RegSz | 3.0.0.10 | 20-00 |
| HelpLink | RegExpandSz | http://www.apple.com/support/ | |
| HelpTelephone | RegSz | 1-800-275-2273 | 00-20-00-50-00-75 |
| InstallDate | RegSz | 20150323 | 02-00 |
| InstallLocation | RegSz | C:\Program Files (x86)\Bonjour\ | 00-6F-00-6E |
| InstallSource | RegSz | C:\Users\NFORM~1\AppData\Local\Temp\XP374.TMP\ | 00-74 |
| ModifyPath | RegExpandSz | MsiExec.exe /X{6E3610B2-430D-4EB0-81E3-2B57E8B9DE8D} | 00-3D |
| NoModify | RegDword | 1 | |
| Publisher | RegSz | Apple Inc. | 00-00-00-53-00-79 |
| Readme | RegSz | | |
| Size | RegSz | | |
| EstimatedSize | RegDword | 2052 | |
| UninstallString | RegExpandSz | MsiExec.exe /X{6E3610B2-430D-4EB0-81E3-2B57E8B9DE8D} | 3B-FE |
| URLInfoAbout | RegSz | http://www.apple.com | 00-75 |
| URLUpdateInfo | RegSz | http://www.apple.com/ | |
| VersionMajor | RegDword | 3 | |
| VersionMinor | RegDword | 0 | |
| WindowsInstaller | RegDword | 1 | |
| Version | RegDword | 50331648 | |
| Language | RegDword | 1033 | |
| DisplayName | RegSz | Bonjour | D0-CF-CF-02 |

Kuvio 22 Bonjour

Drag a column header here to group by that column

| Value Name | Value Type | Data | Value Slack |
|---------------------|-------------|--|-------------|
| AuthorizedCDFPrefix | RegSz | | |
| Comments | RegSz | | |
| Contact | RegSz | | |
| DisplayVersion | RegSz | 4.0.30319 | |
| HelpLink | RegSz | | |
| HelpTelephone | RegSz | | |
| InstallDate | RegSz | 20150325 | E1-02 |
| InstallLocation | RegSz | | |
| InstallSource | RegSz | C:\Users\INFORM~1\AppData\Local\Temp\Microsoft .NET Framework 4 Setup_4.0.30319\ | 00-00 |
| ModifyPath | RegExpandSz | MsiExec.exe /X{8E34682C-8118-31F1-8C4C-98CD9679E1C2} | 00-00 |
| NoModify | RegDword | 1 | |
| NoRepair | RegDword | 1 | |
| Publisher | RegSz | Microsoft Corporation | |
| Readme | RegExpandSz | http://go.microsoft.com/fwlink/?LinkId=164156 | |
| Size | RegDword | 53233 | |
| EstimatedSize | RegDword | 239420 | |
| SystemComponent | RegDword | 1 | |
| UninstallString | RegExpandSz | MsiExec.exe /X{8E34682C-8118-31F1-8C4C-98CD9679E1C2} | 00-00 |
| URLInfoAbout | RegSz | http://go.microsoft.com/fwlink/?LinkId=164164 | |
| URLUpdateInfo | RegSz | http://go.microsoft.com/fwlink/?LinkId=164165 | |
| VersionMajor | RegDword | 4 | |
| VersionMinor | RegDword | 0 | |
| WindowsInstaller | RegDword | 1 | |
| Version | RegDword | 67139183 | |
| Language | RegDword | 0 | |
| DisplayName | RegSz | Microsoft .NET Framework 4 Extended | 00-00-00-00 |

Kuvio 23 Microsoft NET Framework 4

| Value Name | Value Type | Data | Value Slack |
|---------------------|-------------|---|-------------------|
| AuthorizedCDFPrefix | RegSz | | |
| Comments | RegSz | Secure Data Removal for Windows | 00-72-00-65 |
| Contact | RegSz | | |
| DisplayVersion | RegSz | 6.2.2962 | 02-00 |
| HelpLink | RegExpandSz | http://bbs.heidi.ie/viewforum.php?f=30 | 00-69-00-63-00-4B |
| HelpTelephone | RegSz | | |
| InstallDate | RegSz | 20150325 | E2-02 |
| InstallLocation | RegSz | | |
| InstallSource | RegSz | C:\Users\INFORM~1\AppData\Local\Temp\eraserInstallBootstrapper\ | 00-54-00-6F |
| ModifyPath | RegExpandSz | MsiExec.exe /I{C6E287F1-2E47-45F0-8851-94F815CFFB48} | 00-2C |
| Publisher | RegSz | The Eraser Project | 36-47-89-87-81-40 |
| Readme | RegSz | | |
| Size | RegSz | | |
| EstimatedSize | RegDword | 18308 | |
| UninstallString | RegExpandSz | MsiExec.exe /I{C6E287F1-2E47-45F0-8851-94F815CFFB48} | 00-2E |
| URLInfoAbout | RegSz | http://eraser.heidi.ie/ | 00-39-00-33 |
| URLUpdateInfo | RegSz | | |
| VersionMajor | RegDword | 6 | |
| VersionMinor | RegDword | 2 | |
| WindowsInstaller | RegDword | 1 | |
| Version | RegDword | 100797330 | |
| Language | RegDword | 1033 | |
| DisplayName | RegSz | Eraser 6.2.0.2962 | |

Kuvio 24 Eraser

| Nimi | Version | Päivämäärä |
|----------------------|---------------|------------|
| Google Chrome | 41.0.2272.101 | 22.03.2015 |
| Google Update Helper | 1.3.26.9 | 22.03.2015 |
| Google Drive | 2.1.3.127 | 23.03.2015 |

| | | |
|--|----------------|------------|
| Apple Application Support | 3.0.6 | 23.03.2015 |
| Apple Software Update | 2.1.3.127 | 23.03.2015 |
| Microsoft Office Professional Plus 2013 | 15.0.4420.1017 | 22.03.2015 |
| Bonjour | 3.0.0.10 | 23.03.2015 |
| Microsoft .NET Framework 4 | 4.0.30319 | 25.03.2015 |
| Eraser | 6.2.2962 | 25.03.2015 |

5 Verkkoselaimet ja Historia

5.1 Työaseman Web-selaimet

Verkkoselaimet pystyi tarkastamaan kahdella eritavalla, joko katsomalla autopsyn historiasta missä on selaimia, tai NTUSER.DAT hive rekisteristä. Molemmat tavat on toteutettuna. Oletuksena tietenkin oli että Internet Explorer on yksi selaimista. Ensimmäisenä kokeilin katsomalla historiasta, järjestämällä ohjelman mukaan lasevasti. Tuloksina tuli odotettu Internet Explorer, sekä Google Chrome. (Kuvio 25)

| | | | | | | | |
|-----------|--|-------------------------|--|-------------------|-------------------|-------------------------|--------------------------|
| History | https://www.google.com/ | 2015-03-24 23:05:40 EET | https://www.google.com/ | Google | Chrome | www.google.com | 2015_data_leakage_pc.E01 |
| History | https://www.google.com/ | 2015-03-24 23:05:40 EET | https://www.google.com/ | Google | Chrome | www.google.com | 2015_data_leakage_pc.E01 |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | 2015_data_leakage_pc.E01 |
| History | https://www.google.com/#q=security+checkpoint+cd-r | 2015-03-24 23:06:50 EET | https://www.google.com/#q=security+checkpoint+cd-r | security check... | Chrome | www.google.com | 2015_data_leakage_pc.E01 |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | 2015_data_leakage_pc.E01 |
| index.dat | https://online.microsoft.com/favicon.ico | 2015-03-22 15:09:19 EET | | | Internet Explo... | online.microsoft.com | 2015_data_leakage_pc.E01 |
| index.dat | http://download.microsoft.com/download/9/1/1/91176CB7... | 2015-03-22 15:12:54 EET | | | Internet Explo... | download.microsoft.com | 2015_data_leakage_pc.E01 |
| index.dat | http://download.microsoft.com/download/5/C/7/5C7074F0... | 2015-03-22 15:14:40 EET | | | Internet Explo... | download.microsoft.com | 2015_data_leakage_pc.E01 |
| index.dat | http://static-hp-eus.s-msn.com/sc/54/4f1880.ico | 2015-03-22 15:09:03 EET | | | Internet Explo... | static-hp-eus.s-msn.com | 2015_data_leakage_pc.E01 |
| index.dat | System_Deployment_Log_goog...app_86fd5b6b43e66935... | 2015-03-22 15:11:21 EET | | | Internet Explo... | app_86fd5b6b43e66935... | 2015_data_leakage_pc.E01 |

Kuvio 25 historia

Toinen tapa saada selko käytetyistä selaimista ja versioista oli NTUSER.DAT hive rekisterin kautta, joka löytyi autopsystä vol3/Users/Informant alta (Kuvio 26)

/img_2015_data_leakage_pc.E01/vol_vol3/Users/informant

| Name | Modified Time | Change Time | Access Time | Created Time | Size |
|-------------------------------|-------------------------|-------------------------|-------------------------|-------------------------|---------|
| Local Settings | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Music | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:41 EET | 152 |
| My Documents | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| NetHood | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Pictures | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:41 EET | 152 |
| PrintHood | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Recent | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Saved Games | 2015-03-24 20:29:10 EET | 2015-03-24 20:29:10 EET | 2015-03-24 20:29:10 EET | 2015-03-22 16:34:41 EET | 368 |
| Searches | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-22 16:34:55 EET | 56 |
| SendTo | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Start Menu | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Templates | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 48 |
| Videos | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:41 EET | 152 |
| NTUSER.DAT | 2015-03-22 16:34:59 EET | 2015-03-25 17:30:57 EET | 2015-03-25 17:30:58 EET | 2015-03-22 16:34:41 EET | 1048576 |
| ntuser.dat.LOG1 | 2015-03-22 16:34:59 EET | 2015-03-25 17:30:57 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 262144 |
| ntuser.dat.LOG2 | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 0 |
| NTUSER.DAT{016888bd-6c6f-1... | 2015-03-22 16:38:15 EET | 2015-03-22 16:38:15 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 65536 |
| NTUSER.DAT{016888bd-6c6f-1... | 2015-03-22 16:38:15 EET | 2015-03-22 16:38:15 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 524288 |
| NTUSER.DAT{016888bd-6c6f-1... | 2015-03-22 16:38:15 EET | 2015-03-22 16:38:15 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 524288 |
| ntuser.ini | 2015-03-25 15:06:09 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 2015-03-22 16:34:41 EET | 20 |

Properties
View in New Window
Open in External Viewer
View File in Timeline...
Extract File(s)
Search for files with the same MD5 hash
Tag File
Remove File Tag
Add file to hash database

Hex Strings File Metadata Results

Matches on page: - of -

Kuvio 26 NTUSER.DAT

Internet Explorerin versio löytyi NTUSER.DAT hive rekisterin alta Microsoft/Internet Explorer/. Käyttöjärjestelmässä oli käytössä IE9.11 ennen päivitystä ja päivityksen jälkeen versio IE11.0 (Kuvio 27)

Drag a column header here to group by that column

| Value Name | Value Type | Data | Value Slack |
|-------------------|------------|---|-------------|
| MkEnabled | RegDword | Yes | 00-00-00-00 |
| Version | RegSz | 9.11.9600.17691 | 00-00-00-00 |
| Build | RegSz | 99600 | |
| WZVersion | RegSz | 9.11.9600.17691 | 00-00-00-00 |
| IntegratedBrowser | RegDword | 1 | |
| svcSPFWLink | RegSz | http://go.microsoft.com/fwlink/?LinkId=524482 | |
| svcVersion | RegSz | 11.0.9600.17691 | 00-00-00-00 |
| svcUpdateVersion | RegSz | 11.0.17 | 00-00-00-00 |
| svcNumber | RegSz | KB3032359 | |

Type viewer Slack viewer Binary viewer

Value name: svcVersion

Value type: RegSz

Value: 11.0.9600.17691

Raw value: 31-00-31-00-2E-00-30-00-2E-00-39-00-36-00-30-00-30-00-2E-00-31-00-37-00-36-00-39-00-31-00-00-00

Slack: 00-00-00-00

Microsoft/Internet Explorer

Value: svcVersion Collapse all hives

Kuvio 27 IE versio

Google Chromen versio löytyi NTUSER.DAT hive rekisteristä myös, mutta Software/Google/Chrome/BLBeacon/ alta. Google Chromen version oli 41.0.2272.101 (Kuvio 28)

| | | | | |
|--|--|--------------|------------|---------------|
| D:\FORENSIIKKA\Project\Forensiikka_self_assignment\Export\ntuser.dat | | Value Name | Value Type | Data |
| CMI-CreateHive{D43B12B8-09B5-40D6-B4F6-F6DFEB78DAEC} | | | | |
| Software | | | | |
| Google | | | | |
| Chrome | | | | |
| BLBeacon | | | | |
| | | version | RegSz | 41.0.2272.101 |
| | | state | RegDword | 1 |
| | | failed_co... | RegDword | 0 |

Kuvio 28 Google Chrome versio

5.2 Hakemistot ja polut selaushistoriassa

Internet Explorerin hakemisto/polku selaushistoriaan, väliaikaisiin tietoihin, jne löytyivät autopsyllä vol3/Users/Informant/AppData/Local/Microsoft/Windows/kansion alta. Väliaikaiset tiedostot löytyivät Temporary InternetFiles kansion alta (Kuvio 29) ja Internet Explorer historia löytyi History kansion alta (Kuvio 30)

| | | | | | | | | | | | | |
|--|-------------------------|-------------------------|-------------------------|-------------------------|------|------------|-------------|------------|--------|---------|------------|-------------|
| img_2015_data_leakage_pc.E01\vol3\Users\Informant\AppData\Local\Microsoft\Windows\Temporary Internet Files | | | | | | | | | | | | 10 Results |
| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | Meta Addr. | Attr. Addr. |
| [current folder] | 2015-03-23 21:18:25 EET | 2015-03-23 21:18:25 EET | 2015-03-23 21:18:25 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | 553 | 144-6 |
| [parent folder] | 2015-03-23 20:35:59 EET | 2015-03-23 20:35:59 EET | 2015-03-23 20:35:59 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 552 | 144-5 |
| Content.IE5 | 2015-03-22 17:48:43 EET | 2015-03-22 17:48:43 EET | 2015-03-22 17:48:43 EET | 2015-03-22 16:34:57 EET | 56 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | 21788 | 144-5 |
| Content.MSO | 2015-03-23 22:27:52 EET | 2015-03-23 22:27:52 EET | 2015-03-23 22:27:52 EET | 2015-03-23 20:37:52 EET | 48 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | 71148 | 144-6 |
| Content.Outlook | 2015-03-23 21:18:25 EET | 2015-03-23 21:18:25 EET | 2015-03-23 21:18:25 EET | 2015-03-23 21:18:25 EET | 152 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 71156 | 144-1 |
| Content.Word | 2015-03-25 17:24:49 EET | 2015-03-25 17:24:49 EET | 2015-03-25 17:24:49 EET | 2015-03-23 20:37:52 EET | 48 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | 71142 | 144-10 |
| Low | 2015-03-23 19:27:45 EET | 2015-03-25 17:22:07 EET | 2015-03-23 19:27:45 EET | 2015-03-22 16:34:44 EET | 584 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 13981 | 144-1 |
| Virtualized | 2015-03-22 17:09:01 EET | 2015-03-25 17:22:07 EET | 2015-03-22 17:09:01 EET | 2015-03-22 16:34:44 EET | 136 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | 15515 | 144-1 |
| counters.dat | 2015-03-22 17:24:20 EET | 2015-03-22 17:24:20 EET | 2015-03-22 17:24:20 EET | 2015-03-22 17:24:20 EET | 128 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 44295 | 128-1 |
| desktop.ini | 2015-03-22 16:34:57 EET | 2015-03-22 16:34:57 EET | 2015-03-22 16:34:57 EET | 2015-03-22 16:34:57 EET | 67 | Allocated | Allocated | rx-xr-xr-x | 0 | 0 | 21785 | 128-1 |

Kuvio 29 Väliaikaiset tiedostot

| | | | | | | | | | | | | |
|---|-------------------------|-------------------------|-------------------------|-------------------------|------|------------|-------------|------------|--------|---------|------------|-------------|
| img_2015_data_leakage_pc.E01\vol3\Users\Informant\AppData\Local\Microsoft\Windows\History | | | | | | | | | | | | 5 Results |
| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | Meta Addr. | Attr. Addr. |
| [current folder] | 2015-03-22 16:34:57 EET | 2015-03-22 16:34:57 EET | 2015-03-22 16:34:57 EET | 2015-03-22 16:34:41 EET | 344 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | 554 | 144-1 |
| [parent folder] | 2015-03-23 20:35:59 EET | 2015-03-23 20:35:59 EET | 2015-03-23 20:35:59 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 552 | 144-5 |
| History.IE5 | 2015-03-25 16:41:13 EET | 2015-03-25 16:41:13 EET | 2015-03-25 16:41:13 EET | 2015-03-22 16:34:57 EET | 56 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | 21792 | 144-5 |
| Low | 2015-03-22 17:08:58 EET | 2015-03-25 17:22:07 EET | 2015-03-22 17:08:58 EET | 2015-03-22 16:34:44 EET | 256 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 15514 | 144-1 |
| desktop.ini | 2015-03-22 16:34:57 EET | 2015-03-22 16:35:00 EET | 2015-03-22 16:34:57 EET | 2015-03-22 16:34:57 EET | 145 | Allocated | Allocated | rx-xr-xr-x | 0 | 0 | 21791 | 128-1 |

Kuvio 30 IE historia

Google Chromen selaimen tiedot löytyivät autopsyllä polusta vol3/Users/Informant/AppData/Local/Google/User Data/Default/. Google Chromen historia löytyi suoraan kansion alta (Kuvio 31). Chromen Cache esimerkiksi löytyi Cache kansion alta (Kuvio 32).

| img_2015_data_leakage_pc.E01/vol_vol3/Users/Informant/AppData/Local/Google/Chrome/User Data/Default | | | | | | | | | | | | | 55 Resu |
|---|--|-------------------------|-------------------------|-------------------------|-------------------------|--------|------------|-------------|-----------|--------|---------|------------|---------|
| Table | | Thumbnail | | | | | | | | | | | |
| Name | | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | Meta Addr. | |
| <input type="checkbox"/> Current Session | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-24 23:05:38 EET | 2015-03-22 17:11:55 EET | 94811 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 46045 | |
| <input type="checkbox"/> Current Tabs | | 2015-03-24 23:07:20 EET | 2015-03-24 23:07:20 EET | 2015-03-24 23:07:20 EET | 2015-03-22 17:12:05 EET | 31970 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 21842 | |
| <input type="checkbox"/> Extension Cookies | | 2015-03-24 16:12:26 EET | 2015-03-24 16:12:26 EET | 2015-03-24 16:12:26 EET | 2015-03-24 16:12:26 EET | 6144 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 71493 | |
| <input type="checkbox"/> Extension Cookies-journal | | 2015-03-24 16:12:26 EET | 2015-03-24 16:12:26 EET | 2015-03-24 16:12:26 EET | 2015-03-24 16:12:26 EET | 1544 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 71661 | |
| <input type="checkbox"/> Favicons | | 2015-03-24 23:07:00 EET | 2015-03-24 23:07:00 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 63488 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62908 | |
| <input type="checkbox"/> Favicons-journal | | 2015-03-24 23:07:00 EET | 2015-03-24 23:07:00 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 16384 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62912 | |
| <input type="checkbox"/> Google Profile.ico | | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 181623 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62930 | |
| <input type="checkbox"/> History | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 135168 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62906 | |
| <input type="checkbox"/> History Provider Cache | | 2015-03-24 23:07:20 EET | 2015-03-24 23:07:20 EET | 2015-03-22 17:27:28 EET | 2015-03-22 17:12:27 EET | 47175 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 46115 | |
| <input type="checkbox"/> History-journal | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 16384 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62907 | |

Kuvio 31 Google Chrome historia

| /img_2015_data_leakage_pc.E01/vol_vol3/Users/Informant/AppData/Local/Google/Chrome/User Data/Default/Cache | | | | | | | | | | | | | 431 Res |
|--|-----------|-------------------------|-------------------------|-------------------------|-------------------------|----------|------------|-------------|------------|--------|---------|------------|-------------|
| Name | Thumbnail | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | Meta Addr. | Attr. Addr. |
| [current folder] | | 2015-03-24 23:07:19 EET | 2015-03-24 23:07:19 EET | 2015-03-24 23:07:19 EET | 2015-03-22 17:11:53 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 62924 | 144-6 |
| [parent folder] | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-22 17:11:53 EET | 424 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 62886 | 144-5 |
| data_0 | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 118784 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62926 | 128-3 |
| data_1 | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 1843200 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62927 | 128-3 |
| data_2 | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 4202496 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62928 | 128-3 |
| data_3 | | 2015-03-24 23:07:21 EET | 2015-03-24 23:07:21 EET | 2015-03-22 17:11:53 EET | 2015-03-22 17:11:53 EET | 16785408 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 62929 | 128-3 |
| f_000001 | | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 31328 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63625 | 128-3 |
| f_000002 | | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 68994 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63656 | 128-3 |
| f_000003 | | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 2015-03-22 17:11:59 EET | 24524 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63658 | 128-3 |
| f_000004 | | 2015-03-22 17:12:01 EET | 2015-03-22 17:12:01 EET | 2015-03-22 17:12:01 EET | 2015-03-22 17:12:01 EET | 98524 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63570 | 128-3 |
| f_000005 | | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 23836 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63872 | 128-3 |
| f_000006 | | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 21288 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63878 | 128-3 |
| f_000007 | | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 21728 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63877 | 128-3 |
| f_000008 | | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 2015-03-22 17:12:03 EET | 19380 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63919 | 128-3 |
| f_000009 | | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 21521 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63566 | 128-3 |
| f_00000a | | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 40641 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63989 | 128-3 |
| f_00000b | | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 23727 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63990 | 128-3 |
| f_00000c | | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 64917 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 63991 | 128-3 |
| f_00000d | | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 329017 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 64013 | 128-3 |
| f_00000e | | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 2015-03-22 17:12:04 EET | 50729 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 64028 | 128-3 |

Kuvio 32 Google Chrome Cache

5.3 Informantin vierailleet sivustot

Herra Informant vieraili lukuisilla sivuilla, joista muutama nostatti hieman epäilystä, varsinkin google haut aiheista ”data leakage method”, ”leaking confidential information”, ”how to leak a secret” ja ”how to delete data”. Kaikki sivustot, jolla herra Informant vieraili on järjestetty Päivämäärän ja kellon ajan mukaan laskevaksi, jolloin herra informantin liikkeitä on helpompi seurata. Syystä että olin laiska, laitoin pelkät kuvan kaappaukset historiasta, enkä taulukoinut sitä. Kuviot 33-38 sisältävät kaiken historian.

| Table | Thumbnail | | | | | | |
|-------------|--|-------------------------|---|---|--------------|-----------------|--|
| Source File | URL | Date Accessed | Referrer URL | Title | Program Name | Domain | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en | 2015-03-24 23:07:19 EET | https://www.google.com/webhp?hl=en | Google | Chrome | www.google.com | |
| History | https://www.google.com/#q=security+chekpoint+cd+r | 2015-03-24 23:06:50 EET | https://www.google.com/#q=security+chekpoint+cd+r | security checkpoint cd+r - Google Search | Chrome | www.google.com | |
| History | https://www.google.com/ | 2015-03-24 23:05:40 EET | https://www.google.com/ | Google | Chrome | www.google.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | https://www.google.com/ | 2015-03-24 23:05:40 EET | https://www.google.com/ | Google | Chrome | www.google.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | https://www.google.com/ | 2015-03-24 23:05:40 EET | https://www.google.com/ | Google | Chrome | www.google.com | |
| History | https://www.google.com/ | 2015-03-24 23:05:40 EET | https://www.google.com/ | Google | Chrome | www.google.com | |
| History | http://www.bing.com/ | 2015-03-24 23:05:40 EET | http://www.bing.com/ | Bing | Chrome | www.bing.com | |
| History | https://news.google.com/news?pz=1&hl=en&tab=rn | 2015-03-24 21:01:18 EET | https://news.google.com/news?pz=1&hl=en&tab=rn | Google News | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&hl=en&tab=rn | 2015-03-24 21:01:18 EET | https://news.google.com/news?pz=1&hl=en&tab=rn | Google News | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 21:00:57 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Sports | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 21:00:53 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Google News | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 21:00:27 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | World | Chrome | news.google.com | |
| History | https://www.cbsnews.com/news/germanwings-flight-9525-... | 2015-03-24 21:00:04 EET | http://www.cbsnews.com/news/germanwings-flight-9525-... | Germanwings Flight 9525: "Everything is pulverized" - CBS ... | Chrome | www.cbsnews.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 20:59:52 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Google News | Chrome | news.google.com | |

Kuvio 33 historia 1

| | | | | | | | |
|---------|--|-------------------------|--|---|--------|-------------------|--|
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 20:43:47 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 20:22:12 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 20:07:09 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 19:52:06 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 19:37:03 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 19:16:47 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 19:01:45 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 18:46:44 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 18:31:43 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 18:16:41 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 18:01:39 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 17:23:16 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Technology | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 17:22:46 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | World | Chrome | news.google.com | |
| History | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | 2015-03-24 17:22:04 EET | https://news.google.com/news?pz=1&cf=all&ned=us&sid... | Google News | Chrome | news.google.com | |
| History | https://tools.google.com/dpape/drive/thankyou.html?hl=en | 2015-03-23 21:56:28 EET | https://tools.google.com/dpape/drive/thankyou.html?hl=en | Google Drive | Chrome | tools.google.com | |
| History | https://tools.google.com/dpape/drive/index.html?hl=en#e... | 2015-03-23 21:56:19 EET | https://tools.google.com/dpape/drive/index.html?hl=en#e... | Download Google Drive Now - For Free | Chrome | tools.google.com | |
| History | https://www.google.com/drive/download/ | 2015-03-23 21:56:15 EET | https://www.google.com/drive/download/ | Download Google Drive - Free Cloud Storage | Chrome | www.google.com | |
| History | https://www.google.com/drive?sa=t&ct=j&q=&src=s&source... | 2015-03-23 21:56:08 EET | https://www.google.com/drive?sa=t&ct=j&q=&src=s&source... | Google Drive - Cloud Storage & File Backup for Photos, Doc... | Chrome | www.google.com | |
| History | https://www.google.com/webhp?hl=en#hl=en&q=google... | 2015-03-23 21:56:04 EET | https://www.google.com/webhp?hl=en#hl=en&q=google... | google drive - Google Search | Chrome | www.google.com | |
| History | http://support.apple.com/ib/DL1455 | 2015-03-23 21:55:35 EET | http://support.apple.com/ib/DL1455 | iCloud for Windows | Chrome | support.apple.com | |
| History | https://support.apple.com/ib/DL1455 | 2015-03-23 21:55:35 EET | https://support.apple.com/ib/DL1455 | iCloud for Windows | Chrome | support.apple.com | |
| History | http://support.apple.com/ib/DL1455?locale=en_US | 2015-03-23 21:55:35 EET | http://support.apple.com/ib/DL1455?locale=en_US | iCloud for Windows | Chrome | support.apple.com | |
| History | https://support.apple.com/ib/DL1455?locale=en_US | 2015-03-23 21:55:35 EET | https://support.apple.com/ib/DL1455?locale=en_US | iCloud for Windows | Chrome | support.apple.com | |
| History | http://www.icloud.com/icloudcontrolpanel/ | 2015-03-23 21:55:34 EET | http://www.icloud.com/icloudcontrolpanel/ | iCloud | Chrome | www.icloud.com | |
| History | https://www.icloud.com/icloudcontrolpanel/ | 2015-03-23 21:55:34 EET | https://www.icloud.com/icloudcontrolpanel/ | iCloud | Chrome | www.icloud.com | |
| History | http://www.icloud.com/icloudcontrolpanel/ | 2015-03-23 21:55:34 EET | http://www.icloud.com/icloudcontrolpanel/ | iCloud | Chrome | www.icloud.com | |
| History | https://www.icloud.com/icloudcontrolpanel/ | 2015-03-23 21:55:34 EET | https://www.icloud.com/icloudcontrolpanel/ | iCloud | Chrome | www.icloud.com | |
| History | https://www.apple.com/icloud/setup/pc.html | 2015-03-23 21:55:28 EET | https://www.apple.com/icloud/setup/pc.html | Apple - iCloud - Learn how to set up iCloud on all your devi... | Chrome | www.apple.com | |
| History | https://www.apple.com/icloud/ | 2015-03-23 21:55:18 EET | https://www.apple.com/icloud/ | Apple - iCloud - Everything you love, everywhere you go. | Chrome | www.apple.com | |
| History | https://www.google.com/url?sa=t&ct=j&q=&src=s&source... | 2015-03-23 21:55:17 EET | https://www.google.com/url?sa=t&ct=j&q=&src=s&source... | Apple - iCloud - Everything you love, everywhere you go. | Chrome | www.google.com | |

Kuvio 34 historia 2

| | | | | | | |
|---------|---|-------------------------|---|---|--------|-----------------------|
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 21:47:43 EET | https://www.google.com/search?q=information+leakage+... | information leakage cases - Google Search | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 21:47:43 EET | https://www.google.com/search?q=information+leakage+... | information leakage cases - Google Search | Chrome | www.google.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:19:21 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | http://www.forensicswiki.org/wiki/Tools:Data_Recovery | 2015-03-23 20:19:21 EET | http://www.forensicswiki.org/wiki/Tools:Data_Recovery | Tools:Data Recovery - ForensicsWiki | Chrome | www.forensicswiki.org |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:19:17 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | http://en.wikipedia.org/wiki/List_of_data_recovery_software | 2015-03-23 20:19:17 EET | http://en.wikipedia.org/wiki/List_of_data_recovery_software | List of data recovery software - Wikipedia, the free ency... | Chrome | en.wikipedia.org |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:18:46 EET | https://www.google.com/search?q=information+leakage+... | | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:18:43 EET | https://www.google.com/search?q=information+leakage+... | | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:18:30 EET | https://www.google.com/search?q=information+leakage+... | how to recover data - Google Search | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:18:15 EET | https://www.google.com/search?q=information+leakage+... | | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:18:10 EET | https://www.google.com/search?q=information+leakage+... | | Chrome | www.google.com |
| History | https://defcon.org/images/defcon-20/dc-20-presentations... | 2015-03-23 20:18:00 EET | https://defcon.org/images/defcon-20/dc-20-presentations... | | Chrome | defcon.org |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:17:57 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:17:19 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | http://forensicswiki.org/wiki/Arbi-Forensic_Techniques | 2015-03-23 20:17:19 EET | http://forensicswiki.org/wiki/Arbi-Forensic_Techniques | Arbi-Forensic techniques - ForensicsWiki | Chrome | forensicswiki.org |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:17:14 EET | https://www.google.com/search?q=information+leakage+... | anti-forensics - Google Search | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:16:55 EET | https://www.google.com/search?q=information+leakage+... | how to delete data - Google Search | Chrome | www.google.com |
| History | http://nij.gov/topics/forensics/evidence/digital/analysis/pa... | 2015-03-23 20:16:42 EET | http://nij.gov/topics/forensics/evidence/digital/analysis/pa... | Digital Evidence Analysis Tools National Institute of Justice | Chrome | nij.gov |
| History | http://nij.gov/topics/forensics/evidence/digital/pages/welc... | 2015-03-23 20:16:37 EET | http://nij.gov/topics/forensics/evidence/digital/pages/welc... | Digital Evidence and Forensics National Institute of Justice | Chrome | nij.gov |
| History | http://nij.gov/topics/forensics/evidence/digital/pages/welc... | 2015-03-23 20:16:37 EET | http://nij.gov/topics/forensics/evidence/digital/pages/welc... | Digital Evidence and Forensics National Institute of Justice | Chrome | nij.gov |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:16:05 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:15:49 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | http://en.wikipedia.org/wiki/Digital_Forensics | 2015-03-23 20:15:49 EET | http://en.wikipedia.org/wiki/Digital_Forensics | Digital forensics - Wikipedia, the free encyclopedia | Chrome | en.wikipedia.org |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:15:44 EET | https://www.google.com/search?q=information+leakage+... | digital forensics - Google Search | Chrome | www.google.com |
| History | http://www.pcadvisor.co.uk/test-centre/internet/3506734... | 2015-03-23 20:15:32 EET | http://www.pcadvisor.co.uk/test-centre/internet/3506734... | 7 best cloud storage services 2015: Dropbox vs Google Dri... | Chrome | www.pcadvisor.co.uk |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:15:31 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:15:09 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | http://en.wikipedia.org/wiki/Cloud_storage | 2015-03-23 20:15:09 EET | http://en.wikipedia.org/wiki/Cloud_storage | Cloud storage - Wikipedia, the free encyclopedia | Chrome | en.wikipedia.org |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:14:50 EET | https://www.google.com/search?q=information+leakage+... | | Chrome | www.google.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:06:53 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |

Kuvio 35 historia 3

| | | | | | | |
|---------|--|-------------------------|--|--|--------|------------------------|
| History | http://research.microsoft.com/en-us/people/yael/publi... | 2015-03-23 20:06:53 EET | http://research.microsoft.com/en-us/people/yael/publi... | | Chrome | research.microsoft.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:06:27 EET | https://www.google.com/search?q=information+leakage+... | cloud storage - Google Search | Chrome | www.google.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:06:01 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | http://en.wikipedia.org/wiki/Intellectual_property | 2015-03-23 20:06:01 EET | http://en.wikipedia.org/wiki/Intellectual_property | Intellectual property - Wikipedia, the free encyclopedia | Chrome | en.wikipedia.org |
| History | http://www.fbi.gov/about-us/investigate/white-collar/cr/p/r | 2015-03-23 20:05:55 EET | http://www.fbi.gov/about-us/investigate/white-collar/cr/p/r | FBI — Intellectual Property Theft | Chrome | www.fbi.gov |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:05:54 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:05:48 EET | https://www.google.com/search?q=information+leakage+... | how to leak a secret - Google Search | Chrome | www.google.com |
| History | http://www.medapost.com/publications/article/205047/go... | 2015-03-23 20:05:28 EET | http://www.medapost.com/publications/article/205047/go... | Google To Settle 'Data Leakage' Case For \$8.5 Million 07/2... | Chrome | www.medapost.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:05:27 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:05:22 EET | https://www.google.com/search?q=information+leakage+... | intellectual property theft - Google Search | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:05:19 EET | https://www.google.com/search?q=information+leakage+... | information leakage cases - Google Search | Chrome | www.google.com |
| History | https://www.google.com/search?q=information+leakage+... | 2015-03-23 20:05:18 EET | https://www.google.com/search?q=information+leakage+... | information leakage cases - Google Search | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=information+le... | 2015-03-23 20:05:15 EET | https://www.google.com/webhp?hl=en#q=information+le... | | Chrome | www.google.com |
| History | http://www.emirates247.com/business/technology/top-5-s... | 2015-03-23 20:04:54 EET | http://www.emirates247.com/business/technology/top-5-s... | Top 5 sources leaking personal data - Emirates247 | Chrome | www.emirates247.com |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:04:53 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=information+le... | 2015-03-23 20:04:33 EET | https://www.google.com/webhp?hl=en#q=information+le... | | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#hl=en&q=informa... | 2015-03-23 20:03:40 EET | https://www.google.com/webhp?hl=en#hl=en&q=informa... | information leakage cases - Google Search | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=leaking+confid... | 2015-03-23 20:03:31 EET | https://www.google.com/webhp?hl=en#q=leaking+confid... | | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=leaking+confid... | 2015-03-23 20:03:17 EET | https://www.google.com/webhp?hl=en#q=leaking+confid... | | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#hl=en&q=leaking... | 2015-03-23 20:02:44 EET | https://www.google.com/webhp?hl=en#hl=en&q=leaking... | leaking confidential information - Google Search | Chrome | www.google.com |
| History | http://www.sans.org/reading-room/whitepapers/awarenes... | 2015-03-23 20:02:18 EET | http://www.sans.org/reading-room/whitepapers/awarenes... | | Chrome | www.sans.org |
| History | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | 2015-03-23 20:02:17 EET | https://www.google.com/url?sa=t&rc=1&q=8esrc=s&source=... | | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#hl=en&q=data+le... | 2015-03-23 20:02:09 EET | https://www.google.com/webhp?hl=en#hl=en&q=data+le... | data leakage methods - Google Search | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=Enemy+Noethe... | 2015-03-23 19:27:56 EET | https://www.google.com/webhp?hl=en#q=Enemy+Noethe... | Enemy Noether - Google Search | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=Enemy+Noethe... | 2015-03-23 19:27:56 EET | https://www.google.com/webhp?hl=en#q=Enemy+Noethe... | Enemy Noether - Google Search | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=sourced=chrome-instant... | 2015-03-22 17:55:44 EET | https://www.google.com/webhp?hl=en#q=sourced=chrome-instant... | | Chrome | www.google.com |
| History | https://www.google.com/webhp?hl=en#q=sourced=chrome-instant... | 2015-03-22 17:55:40 EET | https://www.google.com/webhp?hl=en#q=sourced=chrome-instant... | | Chrome | www.google.com |
| History | http://tools.google.com/chrome/intl/en/welcome.html | 2015-03-22 17:55:28 EET | http://tools.google.com/chrome/intl/en/welcome.html | Getting Started | Chrome | tools.google.com |
| History | https://www.google.com/intl/en/chrome/browser/welcome... | 2015-03-22 17:55:28 EET | https://www.google.com/intl/en/chrome/browser/welcome... | Getting Started | Chrome | www.google.com |
| History | https://www.google.com/#q=outlook+2013+settings | 2015-03-22 17:28:16 EET | https://www.google.com/#q=outlook+2013+settings | Google | Chrome | www.google.com |

Kuvio 36 historia 4

| | | | | | | |
|---------|---|-------------------------|---|--|--------|------------------------|
| History | https://support.office.com/en-nz/article/Set-up-email-in-O... | 2015-03-22 17:28:13 EET | https://support.office.com/en-nz/article/Set-up-email-in-O... | Set up email in Outlook 2010 or Outlook 2013 for Office 36... | Chrome | support.office.com |
| History | http://tools.google.com/chrome/intl/en/welcome.html | 2015-03-22 17:11:58 EET | http://tools.google.com/chrome/intl/en/welcome.html | Getting Started | Chrome | tools.google.com |
| History | https://www.google.com/intl/en/chrome/browser/welcome... | 2015-03-22 17:11:58 EET | https://www.google.com/intl/en/chrome/browser/welcome... | Getting Started | Chrome | www.google.com |
| History | https://www.google.com/chrome/browser/thankyou.html?... | 2015-03-22 17:11:16 EET | https://www.google.com/chrome/browser/thankyou.html?... | Chrome Browser | Chrome | www.google.com |
| History | https://www.google.com/chrome/index.html?hl=en&brand... | 2015-03-22 17:11:14 EET | https://www.google.com/chrome/index.html?hl=en&brand... | Chrome | Chrome | www.google.com |
| History | https://dl.google.com/update2/1.3.26.9/GoogleInstaller_e... | 2015-03-22 17:11:08 EET | https://dl.google.com/update2/1.3.26.9/GoogleInstaller_e... | | Chrome | dl.google.com |
| History | http://download.microsoft.com/download/7/1/7/7179A150... | 2015-03-22 17:11:06 EET | http://download.microsoft.com/download/7/1/7/7179A150... | | Chrome | download.microsoft.com |
| History | https://www.google.com/search?hl=en&source=hp&q=int... | 2015-03-22 17:10:52 EET | https://www.google.com/search?hl=en&source=hp&q=int... | internet explorer 11 - Google Search | Chrome | www.google.com |
| History | http://windows.microsoft.com/en-us/internet-explorer/do... | 2015-03-22 17:10:50 EET | http://windows.microsoft.com/en-us/internet-explorer/do... | Download Web Browser - Internet Explorer | Chrome | windows.microsoft.com |
| History | http://windows.microsoft.com/en-us/internet-explorer/ie-1... | 2015-03-22 17:09:24 EET | http://windows.microsoft.com/en-us/internet-explorer/ie-1... | Download Internet Explorer 11 (Offline installer) - Internet ... | Chrome | windows.microsoft.com |
| History | http://www.google.com/url?url=http://windows.microsoft... | 2015-03-22 17:09:56 EET | http://www.google.com/url?url=http://windows.microsoft... | | Chrome | www.google.com |
| History | http://www.google.com/url?url=http://windows.microsoft... | 2015-03-22 17:09:52 EET | http://www.google.com/url?url=http://windows.microsoft... | | Chrome | www.google.com |
| History | https://www.google.com/?qws_rd=ssl | 2015-03-22 17:09:40 EET | https://www.google.com/?qws_rd=ssl | Google | Chrome | www.google.com |
| History | http://www.msn.com/?ocid=iehp | 2015-03-22 17:09:24 EET | http://www.msn.com/?ocid=iehp | msn | Chrome | www.msn.com |
| History | http://windows.microsoft.com/en-us/internet-explorer/ie-8... | 2015-03-22 17:09:22 EET | http://windows.microsoft.com/en-us/internet-explorer/ie-8... | Your browser has been upgraded - Microsoft Windows | Chrome | windows.microsoft.com |
| History | http://windows.microsoft.com/en-US/internet-explorer/pro... | 2015-03-22 17:09:20 EET | http://windows.microsoft.com/en-US/internet-explorer/pro... | | Chrome | windows.microsoft.com |
| History | http://go.microsoft.com/fwlink/?LinkID=121792 | 2015-03-22 17:09:20 EET | http://go.microsoft.com/fwlink/?LinkID=121792 | | Chrome | go.microsoft.com |
| History | http://go.microsoft.com/fwlink/?LinkID=69157 | 2015-03-22 17:09:02 EET | http://go.microsoft.com/fwlink/?LinkID=69157 | | Chrome | go.microsoft.com |

Kuvio 37 historia 5

5.4 Informantin käyttämät hakutermit

Autopsy ei näyttänyt kuin murto-osan hakutermeistä joita herra Informant käytti, joten hakuja joutui kalastamaan historian seasta, joka oli erittäin työlästä. Kuvioden jälkeen on taulukko joka sisältää kaikki löytämäni tehdy haut.

| | | | | | |
|-----------|---------------------|----------------------------------|-------------------|-------------------------|--------------------------|
| History | www.google.com | internet explorer 11 | Chrome | 2015-03-22 17:10:52 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | data leakage methods | Chrome | 2015-03-23 20:02:09 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | leaking confidential information | Chrome | 2015-03-23 20:02:44 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:03:40 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:05:18 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:05:19 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:05:22 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:05:48 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:06:27 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:14:50 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:15:44 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:16:55 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:17:14 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:18:10 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:18:15 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:18:30 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:18:43 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 20:18:46 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 21:47:43 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | information leakage cases | Chrome | 2015-03-23 21:47:43 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | google | Chrome | 2015-03-23 21:48:19 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | apple icloud | Chrome | 2015-03-23 21:55:09 EET | 2015_data_leakage_pc.E01 |
| History | www.google.com | google drive | Chrome | 2015-03-23 21:56:04 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | int | Internet Explorer | 2015-03-22 15:09:43 EET | 2015_data_leakage_pc.E01 |
| index.dat | www.google.com | internet explorer 11 | Internet Explorer | 2015-03-22 15:09:48 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | intern | Internet Explorer | 2015-03-22 15:09:44 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | internet explorer 11 | Internet Explorer | 2015-03-22 15:09:46 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | internet e | Internet Explorer | 2015-03-22 15:09:44 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | i | Internet Explorer | 2015-03-22 15:09:43 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | interne | Internet Explorer | 2015-03-22 15:09:44 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | internet ex | Internet Explorer | 2015-03-22 15:09:44 EET | 2015_data_leakage_pc.E01 |

Kuvio 38 haku 1

| | | | | | |
|-----------|---------------------|---------------------|-------------------|-------------------------|--------------------------|
| index.dat | clients1.google.com | internet explorer | Internet Explorer | 2015-03-22 15:09:45 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | internet explorer 1 | Internet Explorer | 2015-03-22 15:09:46 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | inter | Internet Explorer | 2015-03-22 15:09:43 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | inte | Internet Explorer | 2015-03-22 15:09:43 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | in | Internet Explorer | 2015-03-22 15:09:43 EET | 2015_data_leakage_pc.E01 |
| index.dat | clients1.google.com | internet | Internet Explorer | 2015-03-22 15:09:44 EET | 2015_data_leakage_pc.E01 |

Kuvio 39 haku 2

| | |
|--------------------------|---------------------|
| security checkpoint cd-r | 24.03.2015 23.06:50 |
| google drive | 23.03.2015 21.56:04 |
| apple icloud | 23.03.2015 21.55:09 |

| | |
|----------------------------------|---------------------|
| data recovery tools | 23.03.2015 20.19:03 |
| how to recover data | 23.03.2015 20.18:30 |
| system cleaner | 23.03.2015 20.18:10 |
| anti-forensics | 23.03.2015 20.17:14 |
| how to delete data | 23.03.2015 20.16:55 |
| digital forensics | 23.03.2015 20.15:44 |
| cloud storage | 23.03.2015 20.14:50 |
| external device and forensics | 23.03.2015 20.14:11 |
| cd burning method in windows | 23.03.2015 20.13:37 |
| cd burning method | 23.03.2015 20.13:20 |
| windows event logs | 23.03.2015 20.12:35 |
| investigation on windows machine | 23.03.2015 20.11:50 |
| what is windows system artifacts | 23.03.2015 20.10:27 |
| forensic email investigation | 23.03.2015 20.10:03 |
| e-mail investigation | 23.03.2015 20.08:54 |
| dlp drm | 23.03.2015 20.08:31 |
| file sharing and tethering | 23.03.2015 20.07:58 |
| how to leak a secret | 23.03.2015 20.06:27 |
| intellectual property theft | 23.03.2015 20.05:48 |
| information leakage cases | 23.03.2015 20.03:40 |

| | |
|----------------------------------|-------------------------|
| leaking confidential information | 23.03.2015 20.02:44 EET |
| data leakage methods | 23.03.2015 20.02:09 EET |

6 Verkkolevyt ja massamuistit

6.1 Liitetty massamuistit

Liitettyjä massamuisteja oli 2 kpl Sandisk Corp. Cruzer Fit mallia olevaa tikkua, joista toisen ID oli 4C5 30012450531101593 ja toisen 4C530012550531106501. Kiinnitetyt tikut löytyivät helposti autopsystä (Kuvio 40)

| Source File | Date/Time | Device Make | Device Model | Device ID | Data Source | Tags |
|-------------|-------------------------|---------------|-----------------|----------------------|--------------------------|------|
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual Mouse | 7&2a7d3009&0&0001 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual Mouse | 7&2a7d3009&0&0001 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual Mouse | 7&2a7d3009&0&0000 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual Mouse | 7&2a7d3009&0&0000 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual USB Hub | 6&b77da92&0&2 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual USB Hub | 6&b77da92&0&2 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual Mouse | 6&b77da92&0&1 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:36 EET | VMware, Inc. | Virtual Mouse | 6&b77da92&0&1 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:35 EET | | ROOT_HUB | 5&3bb57b&0 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:35 EET | | ROOT_HUB | 5&3bb57b&0 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:35 EET | | ROOT_HUB20 | 5&299e1c9f&0 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-25 15:05:35 EET | | ROOT_HUB20 | 5&299e1c9f&0 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-24 21:38:09 EET | SanDisk Corp. | Cruzer Fit | 4C530012550531106501 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-24 21:38:09 EET | SanDisk Corp. | Cruzer Fit | 4C530012550531106501 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-24 15:38:00 EET | SanDisk Corp. | Cruzer Fit | 4C530012450531101593 | 2015_data_leakage_pc.E01 | |
| SYSTEM | 2015-03-24 15:38:00 EET | SanDisk Corp. | Cruzer Fit | 4C530012450531101593 | 2015_data_leakage_pc.E01 | |

Kuvio 40 kiinnitetyt tikut

Kiinnitetyt tikut voi myös löytää SYSTEM hive rekisterin kautta

ControlSet001/Enum/USBSTOR/Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01/ alta
(Kuvio 41)(Kuvio 42)

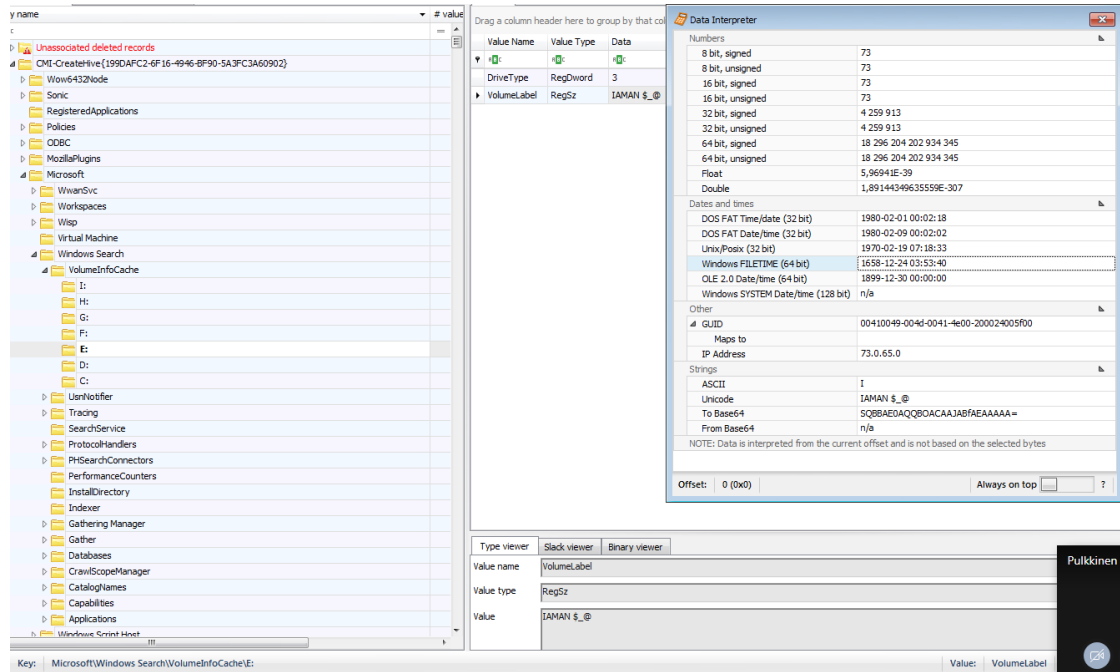
| Value Name | Value Type | Data | Value Slack |
|---------------|------------|--|-------------------|
| DeviceDesc | RegSz | @disk.inf,%disk_devdesc%;Disk drive | 22-00-00-00 |
| Capabilities | RegDword | 16 | |
| HardwareID | RegMultiSz | USBSTOR\DiskSanDisk_Cruzer_Fit____2.01 USBSTOR\DiskSanDisk_Cruzer_Fit____ USBST... | 00-00-00-00 |
| CompatibleIDs | RegMultiSz | USBSTOR\Disk USBSTOR\RAW | |
| ContainerID | RegSz | {4933888a-6002-5a33-95a4-bad21ec52623} | 00-00-00-00-00-00 |
| ConfigFlags | RegDword | 0 | |
| ClassGUID | RegSz | {4d36e967-e325-11ce-bfc1-08002be10318} | 00-00-00-00-00-00 |
| Driver | RegSz | {4d36e967-e325-11ce-bfc1-08002be10318}\0001 | 00-00-00-00 |
| Class | RegSz | DiskDrive | |
| Mfg | RegSz | @disk.inf,%genmanufacturer%;(Standard disk drives) | 87-DA-00-00-00-00 |
| Service | RegSz | disk | 50-00 |
| FriendlyName | RegSz | SanDisk Cruzer Fit USB Device | |

Kuvio 41 4C5 30012450531101593

| Value Name | Value Type | Data | Value Slack |
|---------------|------------|--|-------------------|
| DeviceDesc | RegSz | @disk.inf,%disk_devdesc%;Disk drive | 00-00-00-00 |
| Capabilities | RegDword | 16 | |
| HardwareID | RegMultiSz | USBSTOR\DiskSanDisk_Cruzer_Fit____2.01 USBSTOR\DiskSanDisk_Cruzer_Fit____ USBST... | 00-00-00-00 |
| CompatibleIDs | RegMultiSz | USBSTOR\Disk USBSTOR\RAW | |
| ContainerID | RegSz | {9f935160-3dcc-5a21-a9bc-b9311fd83c43} | 00-00-00-00-00-00 |
| ConfigFlags | RegDword | 0 | |
| ClassGUID | RegSz | {4d36e967-e325-11ce-bfc1-08002be10318} | 00-00-00-00-00-00 |
| Driver | RegSz | {4d36e967-e325-11ce-bfc1-08002be10318}\0002 | 00-00-00-00 |
| Class | RegSz | DiskDrive | |
| Mfg | RegSz | @disk.inf,%genmanufacturer%;(Standard disk drives) | 00-00-00-00-00-00 |
| Service | RegSz | disk | 00-00 |
| FriendlyName | RegSz | SanDisk Cruzer Fit USB Device | |

Kuvio 42 4C530012550531106501

Toinen massamuisteista oli herra Informantin oma, tämä herättää hieman epäilystä sillä yleensä omia tikkuja ei saa tunkea tietokoneisiin työpaikoilla, joissa käsitellään arkaluontoista tietoa. (Kuvio 43)



Kuvio 43 Herra Informantin massamuisti

6.2 NAS IP-osoite

NAS IP-osoite löytyi ntuder.dat rekisterin alta hakemistosta

Software/Microsoft/Windows/CurrentVersion/Explorer/RunMRU (Kuvio 44) NAS palvelimen osoite oli 10.11.11.128

| Value Name | Mru Position | Executable | Opened On |
|------------|--------------|------------------------------|---------------------|
| b | 0 | \\10.11.11.128\secured_drive | 2015-03-23 20:23:28 |
| a | 1 | cmd | |

Kuvio 44 NAS IP osoite

Saman informaation olisi voinut löytää myös autopsyyllä, lähiaikoina käytetyistä dokumenteista. (Kuvio 45)

| Views | Results | Views | Results |
|----------------------------------|---|---|-------------------------|
| 2015_data_leakage_rm#2.E01 | inf.lnk | C:\Windows\inf | 2015-03-22 17:57:31 EET |
| Devices Attached (16) | setupapi.dev.lnk | C:\Windows\inf\setupapi.dev.log | 2015-03-22 17:57:30 EET |
| EXIF Metadata (31) | (secret_project)_pricing_decision.xlsx.LNK | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\prici... | 2015-03-23 22:26:53 EET |
| Encryption Suspected (5) | Desktop.LNK | C:\Users\informant\Desktop | 2015-03-24 20:48:40 EET |
| Extension Mismatch Detected (43) | Resignation_Letter_(Iaman Informant).docx.LNK | C:\Users\informant\Desktop\Resignation_Letter_(Iaman_I... | 2015-03-24 20:48:41 EET |
| Operating System Information (2) | Templates.LNK | C:\Users\informant\AppData\Roaming\Microsoft\Templates | 2015-03-23 20:38:12 EET |
| Recent Documents (24) | (secret_project)_design_concept.LNK | E:\RM#1\Secret Project Data\design\secret_project_desi... | 2015-03-23 20:38:23 EET |
| Web Bookmarks (25) | (secret_project)_final_meeting.pptx.LNK | \\10.11.11.128\secured_drive\Secret Project Data\final[s... | 2015-03-23 22:27:37 EET |
| Web Cookies (371) | (secret_project)_proposal.LNK | E:\RM#1\Secret Project Data\proposal\secret_project_pr... | 2015-03-23 20:37:54 EET |
| Web Downloads (5) | (secret_project)_pricing_decision.xlsx.lnk | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\prici... | 2015-03-23 22:26:53 EET |
| Web History (1339) | CD Drive (2).lnk | D:\ | 2015-03-24 23:01:11 EET |
| Web Search (37) | CD Drive.lnk | D:\ | 2015-03-24 22:47:22 EET |

Kuvio 45 autopsy NAS ip

6.3 Verkkolevyltä avatut tiedostot

Selaamalla Recent hakemistoa, pystyi näkemään juuri äskettäin käytetyt ja avatut tiedostot (Kuvio 46) Recent kansioista löytyi .lnk päätteisiä tiedostoja, eli linkkejä ”avattu tiedosto”. Kansion sisältä löytyi 4 tiedostoa ”pricing_decision”, ”design_concept”, ”final_meeting” ja ”proposal”

| /img_2015_data_leakage_pc.E01/vol_vol3/Users/Informant/AppData/Roaming/Microsoft/Windows/Recent | | | | | | | | | | 20 Results |
|---|-----------|-------------------------|-------------------------|-------------------------|-------------------------|-------|------------|-------------|-------------|------------|
| Table | Thumbnail | | | | | | | | | |
| Name | | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | |
| [current folder] | | 2015-03-25 17:29:08 EET | 2015-03-25 17:29:08 EET | 2015-03-25 17:29:08 EET | 2015-03-22 16:34:41 EET | 176 | Allocated | Allocated | d-wx-wx-wx | |
| [parent folder] | | 2015-03-23 19:27:32 EET | 2015-03-23 19:27:32 EET | 2015-03-23 19:27:32 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | drwxrwxrwx | |
| AutomaticDestinations | | 2015-03-25 17:28:47 EET | 2015-03-25 17:28:47 EET | 2015-03-25 17:28:47 EET | 2015-03-22 16:35:02 EET | 56 | Allocated | Allocated | drwxrwxrwx | |
| CustomDestinations | | 2015-03-25 17:15:54 EET | 2015-03-25 17:15:54 EET | 2015-03-25 17:15:54 EET | 2015-03-22 16:35:01 EET | 56 | Allocated | Allocated | drwxrwxrwx | |
| [secret_project]_pricing_decision.xlsx.lnk | | 2015-03-23 22:26:53 EET | 2015-03-23 22:26:53 EET | 2015-03-23 22:26:53 EET | 2015-03-23 22:26:53 EET | 1952 | Allocated | Allocated | rw-rw-rw-rw | |
| [secret_project]_design_concept.lnk | | 2015-03-23 20:38:21 EET | 2015-03-23 20:38:21 EET | 2015-03-23 20:38:21 EET | 2015-03-23 20:38:21 EET | 13542 | Allocated | Allocated | rw-rw-rw-rw | |
| [secret_project]_final_meeting.pptx.lnk | | 2015-03-23 22:27:33 EET | 2015-03-23 22:27:33 EET | 2015-03-23 22:27:33 EET | 2015-03-23 22:27:33 EET | 793 | Allocated | Allocated | rw-rw-rw-rw | |
| [secret_project]_proposal.lnk | | 2015-03-23 20:37:20 EET | 2015-03-23 20:37:20 EET | 2015-03-23 20:37:20 EET | 2015-03-23 20:37:20 EET | 13475 | Allocated | Allocated | rw-rw-rw-rw | |
| CD Drive (2).lnk | | 2015-03-24 23:01:14 EET | 2015-03-24 23:01:14 EET | 2015-03-24 23:01:14 EET | 2015-03-24 23:01:11 EET | 243 | Allocated | Allocated | rw-rw-rw-rw | |
| CD Drive.lnk | | 2015-03-24 22:47:30 EET | 2015-03-24 22:47:30 EET | 2015-03-24 22:47:30 EET | 2015-03-24 22:47:22 EET | 243 | Allocated | Allocated | rw-rw-rw-rw | |
| desktop.ini | | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:55 EET | 432 | Allocated | Allocated | rw-rw-rw-rw | |
| final.lnk | | 2015-03-23 22:27:33 EET | 2015-03-23 22:27:33 EET | 2015-03-23 22:27:33 EET | 2015-03-23 22:27:33 EET | 555 | Allocated | Allocated | rw-rw-rw-rw | |
| Koala.jpg.lnk | | 2015-03-24 23:01:12 EET | 2015-03-24 23:01:12 EET | 2015-03-24 23:01:12 EET | 2015-03-24 22:47:22 EET | 348 | Allocated | Allocated | rw-rw-rw-rw | |
| Penguins.jpg.lnk | | 2015-03-24 23:01:10 EET | 2015-03-24 23:01:10 EET | 2015-03-24 23:01:10 EET | 2015-03-24 23:01:10 EET | 361 | Allocated | Allocated | rw-rw-rw-rw | |
| pricing_decision.lnk | | 2015-03-23 22:26:54 EET | 2015-03-23 22:26:54 EET | 2015-03-23 22:26:54 EET | 2015-03-23 22:26:54 EET | 1631 | Allocated | Allocated | rw-rw-rw-rw | |
| Resignation_Letter_(taman_informant).docx.lnk | | 2015-03-25 17:29:08 EET | 2015-03-25 17:29:08 EET | 2015-03-25 17:29:08 EET | 2015-03-24 20:48:40 EET | 675 | Allocated | Allocated | rw-rw-rw-rw | |
| Resignation_Letter_(taman_informant).xps.lnk | | 2015-03-25 17:28:33 EET | 2015-03-25 17:28:33 EET | 2015-03-25 17:28:33 EET | 2015-03-25 17:28:33 EET | 602 | Allocated | Allocated | rw-rw-rw-rw | |
| secret.lnk | | 2015-03-23 20:38:21 EET | 2015-03-23 20:38:21 EET | 2015-03-23 20:38:21 EET | 2015-03-23 20:37:20 EET | 11732 | Allocated | Allocated | rw-rw-rw-rw | |
| Tulips.jpg.lnk | | 2015-03-24 23:01:14 EET | 2015-03-24 23:01:14 EET | 2015-03-24 23:01:14 EET | 2015-03-24 22:47:30 EET | 353 | Allocated | Allocated | rw-rw-rw-rw | |
| winter_vhether_advisory.zip.lnk | | 2015-03-24 22:44:18 EET | 2015-03-24 22:44:18 EET | 2015-03-24 22:44:18 EET | 2015-03-24 16:01:23 EET | 453 | Allocated | Allocated | rw-rw-rw-rw | |

Kuvio 46 Recent hakemisto

NTUSER.DAT rekisteristä löytyi, että tiedostot oltiin avattu excelillä(Kuvio47), sekä powerpointilla (Kuvio 48)

| Value Name | Data |
|------------|---|
| Item 1 | [F000000000][T0 ID065A7B4C94EE2][0000000000]*\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\secret_project_pricing_decision.xlsx |

Kuvio 47 Excel lnk

| Value Name | Data |
|------------|---|
| Item 1 | [F000000000][T0 ID065A7CD535A02][0000000000]*\\10.11.11.128\secured_drive\Secret Project Data\final\secret_project_final_meeting.pptx |
| Item 2 | [F000000000][T0 ID065988AED3462][0000000000]*E:\RM#1\Secret Project Data\design\secret_project_design_concept.ppt |

Kuvio 48 Power Point lnk

Myöskin tutkittaessa Officen Roaming profiilia, sieltä löytyi samat linkit, mitä edellä mainittu. (Kuvio 49)

| /img_2015_data_leakage_pc.E01/vol3/Users/Informant/AppData/Roaming/Microsoft/Office/Recent | | | | | | | | | | |
|--|-------------------------|-------------------------|-------------------------|-------------------------|------|------------|-------------|------------|--------|---------|
| Table Thumbnail | | | | | | | | | | |
| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID |
| [current folder] | 2015-03-25 17:28:09 EET | 2015-03-25 17:28:09 EET | 2015-03-25 17:28:09 EET | 2015-03-23 20:37:54 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 |
| [parent folder] | 2015-03-23 20:37:54 EET | 2015-03-23 20:37:54 EET | 2015-03-23 20:37:54 EET | 2015-03-23 19:29:34 EET | 248 | Allocated | Allocated | drwxrwxrwx | 0 | 0 |
| [secret_project]_pricing_decision.xlsx.LNK | 2015-03-23 22:26:56 EET | 2015-03-23 22:26:56 EET | 2015-03-23 22:26:56 EET | 2015-03-23 22:26:53 EET | 1780 | Allocated | Allocated | rwxrwxrwx | 0 | 0 |
| [secret_project]_design_concept.LNK | 2015-03-23 20:38:23 EET | 2015-03-23 20:38:23 EET | 2015-03-23 20:38:23 EET | 2015-03-23 20:38:23 EET | 698 | Allocated | Allocated | rwxrwxrwx | 0 | 0 |
| [secret_project]_final_meeting.pptx.LNK | 2015-03-23 22:27:37 EET | 2015-03-23 22:27:37 EET | 2015-03-23 22:27:37 EET | 2015-03-23 22:27:37 EET | 695 | Allocated | Allocated | rwxrwxrwx | 0 | 0 |
| [secret_project]_proposal.LNK | 2015-03-23 20:37:54 EET | 2015-03-23 20:37:54 EET | 2015-03-23 20:37:54 EET | 2015-03-23 20:37:54 EET | 687 | Allocated | Allocated | rwxrwxrwx | 0 | 0 |
| Desktop.LNK | 2015-03-24 20:48:40 EET | 2015-03-24 20:48:40 EET | 2015-03-24 20:48:40 EET | 2015-03-24 20:48:40 EET | 851 | Allocated | Allocated | rwxrwxrwx | 0 | 0 |
| index.dat | 2015-03-25 17:28:09 EET | 2015-03-25 17:28:09 EET | 2015-03-23 20:37:54 EET | 2015-03-23 20:37:54 EET | 478 | Allocated | Allocated | rw-r--r-- | 0 | 0 |
| Resignation_Letter_(Iaman_Informant).docx.LNK | 2015-03-23 20:38:12 EET | 2015-03-23 20:38:12 EET | 2015-03-25 17:28:09 EET | 2015-03-24 20:48:41 EET | 1133 | Allocated | Allocated | rwxrwxrwx | 0 | 0 |
| Templates.LNK | 2015-03-23 20:38:12 EET | 2015-03-23 20:38:12 EET | 2015-03-23 20:38:12 EET | 2015-03-23 20:38:12 EET | 1099 | Allocated | Allocated | rwxrwxrwx | 0 | 0 |

Kuvio 49 Office roaming profiili

Samat tiedostot, pystyi näkemään myös autopsyn recent files tabista (Kuvio 48), mutta ilman tarkempaa tietoa siitä, mitkä ohjelmat käyttivät ja milloinkin.

| | | | |
|--|---|-------------------------|--------------------------|
| [secret_project]_final_meeting.pptx.LNK | \\10.11.11.128\secured_drive\Secret Project Data\final[s... | 2015-03-23 22:27:37 EET | 2015_data_leakage_pc.E01 |
| [secret_project]_final_meeting.pptx.lnk | \\10.11.11.128\secured_drive\Secret Project Data\final[s... | 2015-03-23 22:27:33 EET | 2015_data_leakage_pc.E01 |
| final.lnk | \\10.11.11.128\secured_drive\Secret Project Data\final | 2015-03-23 22:27:33 EET | 2015_data_leakage_pc.E01 |
| [secret_project]_pricing_decision.xlsx.LNK | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\prici... | 2015-03-23 22:26:53 EET | 2015_data_leakage_pc.E01 |
| [secret_project]_pricing_decision.xlsx.lnk | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\prici... | 2015-03-23 22:26:53 EET | 2015_data_leakage_pc.E01 |
| pricing decision.lnk | \\10.11.11.128\SECURED_DRIVE\Secret Project Data\prici... | 2015-03-23 22:26:54 EET | 2015_data_leakage_pc.E01 |
| secret.lnk | No preferred path found | 2015-03-23 20:37:20 EET | 2015_data_leakage_pc.E01 |
| [secret_project]_proposal.LNK | E:\RM#1\Secret Project Data\proposal[secret_project]_pr... | 2015-03-23 20:37:54 EET | 2015_data_leakage_pc.E01 |
| [secret_project]_proposal.lnk | E:\RM#1\Secret Project Data\proposal[secret_project]_pr... | 2015-03-23 20:37:20 EET | 2015_data_leakage_pc.E01 |
| [secret_project]_design_concept.LNK | E:\RM#1\Secret Project Data\design[secret_project]_desi... | 2015-03-23 20:38:23 EET | 2015_data_leakage_pc.E01 |
| [secret_project]_design_concept.lnk | E:\RM#1\Secret Project Data\design[secret_project]_desi... | 2015-03-23 20:38:21 EET | 2015_data_leakage_pc.E01 |

Kuvio 50 autopsy recent tab

6.4 Pilvipalveluihin liittyvät jäljet

Informantin AppData kansion alta löytyi Google Driven sync konfigurointi tiedosto, jonka sähköpostikäyttäjä on iaman.informant.personal@gmail.com Google Drive synkronointia varten (Kuvio 51)

Sync_log.log tutkimisen jälkeen löytyi tietoa siitä, että Google Drive käyttäjä oli tehty
23.03.2015 16.05:32 GMT (Kuvio 52)

| sync_log.log | 2015-03-25 17:23:00 EET | 2015-03-25 17:23:00 EET | 2015-03-23 22:02:51 |
|--------------|-------------------------|-------------------------|---------------------|
| sync_log.log | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |

Hex

Strings

File Metadata

Results

Message

Indexed Text

Media

Other Occurrences

Matches on page: - of - Match











Page: 1 of 14 Page

```








pdating local entry inode=844424930207017, filename=\\?C:\Users\informant\Google Drive
2015-03-23 16:05:32,265 -0400 INFO pid=2576 2828:LaunchThreads common.persistence.snapshot_sqlite:171 A
dding cloud entry resource_id=folder:root, filename=None
2015-03-23 16:05:32,265 -0400 INFO pid=2576 2828:LaunchThreads common.persistence.snapshot_sqlite:248 U
pdating cloud entry doc_id=root, filename=root
2015-03-23 16:05:32,265 -0400 INFO pid=2576 2828:LaunchThreads common.persistence.snapshot_sqlite:518 A
dding Mapping inode=844424930207017, doc_id=root
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads common.service.user:64 Initializing User
instance with new credentials. iaman.informant.personal@gmail.com
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads common.sync.app:1153 Feature Switches:

```

Program Files(x86) alta löytyi myös Google Drive sync DLL tiedostot (Kuvio 53) ja Download kansista löytyi .exe tiedostot Google Driven ja Icloudin asentamiseen (Kuvio 54).

| img_2015_data_leakage_pc.E01/vol_vol3/Program Files (x86)/Google/Drive | | | | | | | | | | | | 10 Results |
|---|-------------------------|-------------------------|-------------------------|-------------------------|----------|------------|-------------|------------|--------|---------|-----------|------------|
| Table | Thumbnail | | | | | | | | | | | |
| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | Meta Addr | |
|  [current folder] | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:43 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 74432 | |
|  [parent folder] | 2015-03-23 22:02:43 EET | 2015-03-23 22:02:43 EET | 2015-03-23 22:02:43 EET | 2015-03-22 17:11:26 EET | 552 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 63040 | |
|  Languages | 2015-03-23 22:02:43 EET | 2015-03-23 22:02:43 EET | 2015-03-23 22:02:43 EET | 2015-03-23 22:02:43 EET | 152 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 74436 | |
|  Microsoft.VC90.ATL | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:43 EET | 400 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 74433 | |
|  Microsoft.VC90.CRT | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 74558 | |
|  Microsoft.VC90.MFC | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | 74552 | |
|  contextmenu64.dll | 2015-02-19 20:24:28 EET | 2015-03-23 22:02:43 EET | 2015-03-23 22:02:43 EET | 2015-02-19 20:24:28 EET | 141128 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | 74435 | |
|  googledrivesync.exe | 2015-02-19 20:24:24 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-02-19 20:24:24 EET | 26232152 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | 74550 | |
|  googledrivesync64.dll | 2015-02-19 20:24:26 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-02-19 20:24:26 EET | 774472 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | 74551 | |
|  nativeproxy.exe | 2015-02-19 20:19:00 EET | 2015-03-23 22:02:44 EET | 2015-03-23 22:02:44 EET | 2015-02-19 20:19:00 EET | 77640 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | 74564 | |

Kuvio 53 Program files Google Drive

| img_2015_data_leakage_pc.E01/vol3/Users/informant/Downloads | | | | | | | | | | | 7 Results |
|---|-------------------------|-------------------------|-------------------------|-------------------------|----------|------------|-------------|------------|--------|---------|-----------|
| Table | Thumbnail | | | | | | | | | | |
| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | |
|  [current folder] | 2015-03-23 21:56:53 EET | 2015-03-23 21:56:53 EET | 2015-03-23 21:56:53 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | d-wx-wx-wx | 0 | 0 | |
|  [parent folder] | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 2015-03-22 16:34:31 EET | 256 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | |
|  desktop.ini | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 2015-03-22 16:34:55 EET | 282 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |
|  googledrivesync.exe | 2015-03-23 21:56:33 EET | 2015-03-23 21:56:33 EET | 2015-03-23 21:56:30 EET | 2015-03-23 21:56:30 EET | 880208 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |
|  googledrivesync.exe:Zone.Identifier | 2015-03-23 21:56:33 EET | 2015-03-23 21:56:33 EET | 2015-03-23 21:56:30 EET | 2015-03-23 21:56:30 EET | 26 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |
|  idoudsetup.exe | 2015-03-23 21:56:53 EET | 2015-03-23 21:56:53 EET | 2015-03-23 21:55:47 EET | 2015-03-23 21:55:47 EET | 71647536 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |
|  idoudsetup.exe:Zone.Identifier | 2015-03-23 21:56:53 EET | 2015-03-23 21:56:53 EET | 2015-03-23 21:55:47 EET | 2015-03-23 21:55:47 EET | 26 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |

Kuvio 54 Downloads kansio

6.5 Google Drivesta poistettut tiedostot

Snapshot.db tiedostoa tarkastelemalla pohjalta löytyi 3 tiedostoa, jotka oli poistettu

Google Drivesta. (Kuvio 56)

img_2015_data_leakage_pc.E01/vol3/Users/informant/AppData/Local/Google/Drive/User_default

18 Results

| Table | Thumbnail | | | | | | | | | | | |
|-----------------------------------|-----------|-------------------------|-------------------------|-------------------------|-------------------------|-------|-------------|-------------|------------|--------|---------|--|
| Name | | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | |
| [current folder] | | 2015-03-25 17:22:48 EET | 2015-03-25 17:22:48 EET | 2015-03-25 17:22:48 EET | 2015-03-23 22:02:51 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | |
| [parent folder] | | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:45 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | |
| cloud_graph | | 2015-03-25 17:22:47 EET | 2015-03-25 17:22:47 EET | 2015-03-25 17:22:47 EET | 2015-03-23 22:05:32 EET | 152 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | |
| CrashReports | | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 48 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | |
| cacerts | | 2015-03-25 17:21:34 EET | 2015-03-25 17:21:34 EET | 2015-03-25 17:21:34 EET | 2015-03-23 22:02:51 EET | 3245 | Unallocated | Unallocated | rw-rw-rw- | 0 | 0 | |
| cacerts | | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 3245 | Unallocated | Unallocated | rw-rw-rw- | 0 | 0 | |
| com.google.drive.nativeproxy.json | | 2015-03-25 17:21:36 EET | 2015-03-25 17:21:36 EET | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 294 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |
| lockfile | | 2015-03-25 17:21:34 EET | 2015-03-25 17:21:34 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 0 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |
| pid | | 2015-03-25 17:21:34 EET | 2015-03-25 17:21:34 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 4 | Allocated | Allocated | rw-rw-rw- | 0 | 0 | |
| run_dir | | 2015-03-25 17:21:34 EET | 2015-03-25 17:21:34 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 46 | Allocated | Allocated | drwxrwxrwx | 0 | 0 | |
| snapshot.db | | 2015-03-25 17:22:48 EET | 2015-03-25 17:22:48 EET | 2015-03-23 22:02:51 EET | 2015-03-23 22:02:51 EET | 20480 | Unallocated | Unallocated | rw-rw-rw- | 0 | 0 | |
| snapshot.db-shm | | 2015-03-25 17:22:48 EET | 2015-03-25 17:22:48 EET | 2015-03-25 17:22:48 EET | 2015-03-25 17:21:34 EET | 32768 | Unallocated | Unallocated | rw-rw-rw- | 0 | 0 | |

Hex

Strings

File Metadata

Results

Message

Indexed Text

Media

Other Occurrences

Matches on page: - of - Match

Page: 1 of 1 Page

Text Source: File Text

```
SOCA
SEARCHFILTERSHOT.EXE
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\WTL11.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\KERNEL32.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\APISETSCHEMA.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\KERNELBASE.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\LOCALI18N.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\SEARCHFILTERSHOT.EXE
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\ADVAPI32.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\MSVCRT.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\SECCHOST.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\RPCRT4.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\USER32.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\OLE32.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\LINK.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\OSF10.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\OLE32.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\OLEAUT32.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\TQUERY.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\SHELLAPI.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\USER32.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\MSCTF.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\MSHOOKS.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\SYSTEM32\\MSCOREE.DLL
\\DEVICE\\HARDISKVOLUME2\\WINDOWS\\MICROSOFT.NET\\FRAMEWORK64\\V4.0.30215\\MSCOREE1.DLL
```

Kuvio 55 Snapshot.db 1

```

\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\RPCSS.DLL
\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CRYPTBASE.DLL
\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CLBCATQ.DLL
\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CRYPTSP.DLL
\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\RSAENH.DLL
\DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\RPCRTREMOTE.DLL
\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\MSSPRXY.DLL
\DEVICE\HARDDISKVOLUME2
\DEVICE\HARDDISKVOLUME2\WINDOWS
-\DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION
5\DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING
-\DEVICE\HARDDISKVOLUME2\WINDOWS\MICROSOFT.NET
9\DEVICE\HARDDISKVOLUME2\WINDOWS\MICROSOFT.NET\FRAMEWORK64
D\DEVICE\HARDDISKVOLUME2\WINDOWS\MICROSOFT.NET\FRAMEWORK64\V4.0.30319
(\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32
OWS\SYSW
local_relations_parent_inode_number_idxlocal_relations
CREATE INDEX local_relations_parent_inode_number_idx on local_relations (parent_inode_number)
tablemappingmapping
CREATE TABLE mapping (inode_number INTEGER, doc_id TEXT, UNIQUE (inode_number), FOREIGN KEY (inode_number
) REFERENCES local_entry(inode_number), FOREIGN KEY (doc_id) REFERENCES cloud_entry(doc_id))-
indexsqlite_autoindex_mapping_1mapping
indexmapping_doc_id_idxmapping
CREATE INDEX mapping_doc_id_idx on mapping (doc_id)
\\?\C:\Users\informant\Google Drive\happy_holiday.jpg
\\?\C:\Users\informant\Google Drive\do_u_wanna_build_a_snow_man.mp3
w \\?\C:\Users\informant\Google Drive\happy_holiday.jpgG
\\?\C:\Users\informant\Google Drive\do_u_wanna_build_a_snow_man.mp3

```

Kuvio 56 Snapshot.db 2

Google Drivesta oli poistettu do_u_wanna_build_a_snow_man.mp3 2 kertaa ja happy_holiday.jpgG tiedostot.

6.6 Herra Informantin irtisanoutuminen

Herra informantin word dokumentti irtisanoutumisesta löytyi työpöydältä mistä aina kaikki asiat löytyvät. Word dokumentti oli muunneltu xps muotoon, mutta ei koskaan tulostettu sillä oikeata printteriä ei ollut ilmeisesti käytössä. Herra Informant kuvitteellisesti tulosti paperin 17.28:34 EET (Kuvio 57)

| /img_2015_data_leakage_pc.E01/vol3/Users/Informant/Desktop | | | | | | | | | | 9 Results |
|--|-----------|-------------------------|-------------------------|-------------------------|-------------------------|--------|-------------|-------------|------------|-----------|
| Table | Thumbnail | | | | | | | | | |
| Name | | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID |
| [current folder] | | 2015-03-25 17:29:08 EET | 2015-03-25 17:29:08 EET | 2015-03-25 17:29:08 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | d-wx-wx-wx | 0 |
| [parent folder] | | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 2015-03-22 16:34:31 EET | 256 | Allocated | Allocated | drwxrwxrwx | 0 |
| [QAT] | | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:49 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 48 | Unallocated | Unallocated | drwxrwxrwx | 0 |
| Download | | 2015-03-25 17:15:45 EET | 2015-03-25 17:15:45 EET | 2015-03-25 17:15:45 EET | 2015-03-22 17:08:23 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 |
| desktop.ini | | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:59 EET | 2015-03-22 16:34:55 EET | 282 | Allocated | Allocated | rw-rw-r-- | 0 |
| Google Drive.lnk | | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 2015-03-23 22:05:32 EET | 1665 | Unallocated | Unallocated | rw-rw-rw-r | 0 |
| Resignation_Letter_(Iaman_Informant).docx | | 2015-03-24 20:59:30 EET | 2015-03-24 20:59:30 EET | 2015-03-24 20:59:30 EET | 2015-03-24 20:48:40 EET | 11893 | Allocated | Allocated | rw-rw-rw-r | 0 |
| Resignation_Letter_(Iaman_Informant).xps | | 2015-03-25 17:28:34 EET | 2015-03-25 17:28:47 EET | 2015-03-25 17:28:33 EET | 2015-03-25 17:28:33 EET | 178139 | Allocated | Allocated | rw-rw-rw-r | 0 |
| ~\$signation_Letter_(Iaman_Informant).docx | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | | ----- | 0 |

Kuvio 57 Irtisanoutuminen

6.7 Roskakori

Roskakorin sisältä löytyi lukuisia asioita, jotka on listattu erikseen bullet pointeilla.

Roskakorin roskien sisällön tietoihin pääsi käsiksi tutkimalla jokaista yksi kerrallaan ja tarkastalemalla sisältöä. Roskakorin sisällä oli paljon tavaraa (Kuvio 58).

| img_2015_data_leakage_pc.E01\vol_vol3\Recycle.Bin\5-1-5-21-2425377081-3129163575-2985601102-1000 | | | | | | | | | | | 29 Results |
|--|-------------------------|-------------------------|-------------------------|--------------------------|------|-------------|-------------|------------|--------|---------|------------|
| Table | Thumbnail | | | | | | | | | | |
| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | |
| [current folder] | 2015-03-25 17:14:45 EET | 2015-03-25 17:14:45 EET | 2015-03-25 17:14:45 EET | 2015-03-22 16:34:46 EET | 56 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | |
| [parent folder] | 2015-03-22 17:56:00 EET | 2015-03-22 17:56:00 EET | 2015-03-22 17:56:00 EET | 2009-07-14 06:18:56 EEST | 56 | Allocated | Allocated | dr-xr-xr-x | 0 | 0 | |
| ✖ \$!40295N | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!508CBB.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!552163 | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!8YP3KK.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!9M7UMY | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!DOI3HE.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!FVCH5V.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!I3FM2A.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!IQGWTT.ini | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!JEMT64.exe | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!IOD1U3.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!U3FKV1.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!X538VH.jpg | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 2015-03-24 22:11:42 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$!XWGVWC | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 2015-03-24 21:51:47 EET | 544 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$R508CBB.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:39 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$R8YP3KK.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:48 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$ROI3HE.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:49 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$RFVCH5V.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:49 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$R13FM2A.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:39 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$RIQGWTT.ini | 2015-03-24 21:57:20 EET | 2015-03-24 22:11:42 EET | 2015-03-24 21:57:20 EET | 2015-03-22 16:35:02 EET | 174 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$RJEMT64.exe | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:48 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$RJEMT64.exe:Zone.Identifier | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:48 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 26 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$ROID1U3.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:39 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$R13FM2A.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:49 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| ✖ \$RX538VH.jpg | 2076-11-29 10:54:34 EET | 2015-03-25 17:13:49 EET | 2076-11-29 10:54:34 EET | 2076-11-29 10:54:34 EET | 0 | Unallocated | Unallocated | rw-rw-rw-r | 0 | 0 | |
| desktop.ini | 2015-03-22 16:34:46 EET | 2015-03-22 16:34:46 EET | 2015-03-22 16:34:46 EET | 2015-03-22 16:34:46 EET | 129 | Allocated | Allocated | rw-rw-rw-r | 0 | 0 | |
| ✖ desktop.ini | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | Unallocated | ----- | 0 | 0 | |

- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\tr
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini

- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\IE11-Windows6.1-x64-en-us.exe
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg
- C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog

6.8 Työasemalta kopioidut tiedostot massamuistille

Massamuistille oli kopioitu lukuisia salaisia tiedostoja, jotka oli uudelleen nimetty, sekä niille oltiin vaihdettu myös formaattia. (Kuvio 59)(Kuvio60) diary 3 on oikeasti technical review3.ppt ja my_friends.svg on oikeasti Progress.doc

| /img_2015_data_leakage_rm#2.E01/vol_v02/\$OrphanFiles/proposal | | | | | | | | | | 4 Results |
|--|--|-------------------------|---------------------|-------------------------|-------------------------|----------|-------------|-------------|------------|-----------|
| Name | Location | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | |
| .. | /img_2015_data_leakage_rm#2.E01/vol_v02/\$OrphanFiles... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | Allocated | v----- | |
| [current folder] | | 2015-03-24 08:55:18 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:44 EET | 4096 | Unallocated | Unallocated | drwxrwxrwx | |
| a_gift_from_you.gif | | 2014-12-18 17:50:58 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:44 EET | 35226880 | Unallocated | Unallocated | rw-rw-rw- | |
| landscape.png | | 2014-12-19 15:53:46 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:05 EET | 6484502 | Unallocated | Unallocated | rw-rw-rw- | |

Kuvio 58 proposal

| /img_2015_data_leakage_rm#2.E01/vol_v02/\$OrphanFiles/TECHNI~1 | | | | | | | | | | 8 Results |
|--|--|-------------------------|---------------------|-------------------------|-------------------------|---------|-------------|-------------|------------|-----------|
| Name | Location | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | User |
| .. | /img_2015_data_leakage_rm#2.E01/vol_v02/\$OrphanFiles... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | Allocated | v----- | 0 |
| [current folder] | | 2015-03-24 08:56:22 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:12 EET | 4096 | Unallocated | Unallocated | drwxrwxrwx | 0 |
| dary_#1d.txt | | 2015-01-05 17:01:08 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:12 EET | 121441 | Unallocated | Unallocated | rw-rw-rw- | 0 |
| dary_#1p.txt | | 2015-01-05 15:15:08 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:12 EET | 458267 | Unallocated | Unallocated | rw-rw-rw- | 0 |
| dary_#2d.txt | | 2015-01-12 17:25:40 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:13 EET | 658922 | Unallocated | Unallocated | rw-rw-rw- | 0 |
| dary_#2p.txt | | 2015-01-12 15:20:26 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:14 EET | 1154560 | Unallocated | Unallocated | rw-rw-rw- | 0 |
| dary_#3d.txt | | 2015-01-20 16:05:00 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:15 EET | 2360832 | Unallocated | Unallocated | rw-rw-rw- | 0 |
| dary_#3p.txt | | 2015-01-20 14:18:06 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 09:00:18 EET | 325120 | Unallocated | Unallocated | rw-rw-rw- | 0 |

| | | | | | | | |
|-----|---------|---------------|---------|---------|--------------|-------|-------------------|
| Hex | Strings | File Metadata | Results | Message | Indexed Text | Media | Other Occurrences |
|-----|---------|---------------|---------|---------|--------------|-------|-------------------|

Matches on page: - of - Match Page: 1 of 1 Page

Text Source: File Text

```
[Secure Project]

technical_review_f3.ppt
This file is one of Gordoco (http://digitalcoopers.org/coopers/gordoco)
The first page is added by NIST CF&DS project.
All following pages have no connection with to the scenario.

SURVIVAL SIGNALS
LISTENING TO YOUR INTUITION
Cheryl L. Wieser
Regional Security Offices
Western Region Security Office
Seattle, WA
206-526-6683
Updated 12/12/2001

FORCED TEAMING

USE OF WORD "WE"
ESTABLISH RAPPORT
ESTABLISH FIDELITY TRUST
PROJECTION OF SHARED PREDICAMENT
DONE IN A REMOTE OR ISOLATED AREA
```

Kuvio 59 diary.txt

img_2015_data_leakage_rm#2.E01\vol_vol2\OrphanFiles\progress 5 Results

| Name | Location | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode |
|-----------------------|--|-------------------------|---------------------|-------------------------|-------------------------|---------|-------------|-------------|------------|
| .. | /img_2015_data_leakage_rm#2.E01\vol_vol2\OrphanFile... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | Allocated | v----- |
| [current folder] | | 2015-03-24 08:54:54 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:43 EET | 4096 | Unallocated | Unallocated | drwxrwxrwx |
| my_friends.svg | | 2015-01-20 11:13:44 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:43 EET | 58368 | Unallocated | Unallocated | rw-rw-rw-r |
| my_smartphone.png | | 2015-01-05 11:57:22 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:43 EET | 4440235 | Unallocated | Unallocated | rw-rw-rw-r |
| new_year_calendar.one | | 2015-01-12 14:23:42 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:44 EET | 27414 | Unallocated | Unallocated | rw-rw-rw-r |

Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences

Matches on page: - of - Match Page: 1 of 1 Page

Text Source: File Text

[Secret Project]
Progress #3.doc
This file is one of Gordocx (<http://digitalcorpora.org/corpora/gordocx>)
The first page is added by NIST CFReD project.
All following pages have no connection with the scenario.
Before the
United States Department of Commerce
National Telecommunications and Information Administration
Washington, D.C. 20230
In Re:
United States Spectrum Management Policy For the 21st Century
Docket No. 040127027402701
Comments of Wayne Longman
The Administration (NTIA) is to be congratulated for this timely and critical initiative on spectrum poli
ry reform. The recent FCC activity to promote unlicensed and unregulated use of the spectrum can only as
tify ad hoc spectrum uses and users where the presence of destructive interference is of short term impa
ct and concern. This is a very limited slice of the needs of the vast majority of spectrum applications
that require near-absolute certainty for interference-free, economical, reliable, and predictable provision
of service. Although the "traditional" spectrum management system provides these certainties, it is a
lso clearly guilty of failing to respond in a rational and timely manner to new and emerging demands on t
he spectrum. It is argued here that these shortcomings are largely institutional in nature and can be r

Kuvio 60 Progress

img_2015_data_leakage_rm#2.E01\vol_vol2\OrphanFiles\PRICIN=1 6 Results

| Name | Location | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode |
|-----------------------|--|-------------------------|---------------------|-------------------------|-------------------------|----------|-------------|-------------|------------|
| .. | /img_2015_data_leakage_rm#2.E01\vol_vol2\OrphanFile... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | Allocated | v----- |
| [current folder] | | 2015-03-24 08:57:32 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:39 EET | 4096 | Unallocated | Unallocated | drwxrwxrwx |
| my_favorite_cars.db | | 2015-01-16 15:10:24 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:39 EET | 1260544 | Unallocated | Unallocated | rw-rw-rw-r |
| my_favorite_movies.7z | | 2015-01-08 17:08:24 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:39 EET | 100078 | Unallocated | Unallocated | rw-rw-rw-r |
| new_years_day.jpg | | 2014-12-01 14:50:26 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:39 EET | 10237535 | Unallocated | Unallocated | rw-rw-rw-r |
| super_bowl.avi | | 2014-12-02 13:28:58 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:40 EET | 10289152 | Unallocated | Unallocated | rw-rw-rw-r |

Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences

Matches on page: - of - Match Page: 1 of 16 Page

Text Source: File Text

NIST
[Secret Project]
price_analysis_#2.xls
This file is one of Gordocx (<http://digitalcorpora.org/corpora/gordocx>)
The first sheet is added by NIST CFReD project.
All following sheets have no connection with the scenario.
ZERNERCO_OH
table with column headers in row 5
Residence County to Workplace County Flows for Ohio
Sorted by Workplace State and County
Res State Res County Res (C)MSA Res FMSA Residence State* County Name Work Stat
21 019 9999 9999 Workplace State*County Name Count
9999 Adams Co. OH 14 Boyd Co. KY 039 001 9999
21 023 9999 9999 Breacken Co. KY 039 001
9999 9999 Adams Co. OH 1
21 043 9999 9999 Carter Co. KY 039 001
9999 9999 Adams Co. OH 54
21 063 9999 9999 Elliott Co. KY 039 001
9999 9999 Adams Co. OH 6
21 069 9999 9999 Fleming Co. KY 039 001
9999 9999 Adams Co. OH 28
21 059 9999 9999 Greenup Co. KY 039 001
9999 9999 Adams Co. OH 8
21 034 9999 9999 Greenup Co. KY 039 001

Kuvio 61 PRICIN

| img_2015_data_leakage_rm#2.E01/vol_v02/\$OrphanFiles/design | | | | | | | | | | 4 Results |
|---|---|-------------------------|---------------------|-------------------------|-------------------------|----------|-------------|-------------|------------|-----------|
| Table Thumbnail | | | | | | | | | | |
| Name | Location | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | |
| .. | /img_2015_data_leakage_rm#2.E01/vol_v02/\$OrphanFile... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | Allocated | v----- | |
| [current folder] | | 2015-03-24 08:57:14 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:26 EET | 4096 | Unallocated | Unallocated | drwxrwxrwx | |
| winter_storm.amr | | 2015-01-23 16:47:10 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:27 EET | 14547968 | Unallocated | Unallocated | rwxrwxrwx | |
| winter_whether_advisory.zip | | 2014-12-16 12:10:26 EET | 0000-00-00 00:00:00 | 2015-03-23 23:00:00 EET | 2015-03-24 08:59:37 EET | 16381123 | Unallocated | Unallocated | rwxrwxrwx | |

| | | | | | | | |
|-----|---------|---------------|---------|---------|--------------|-------|-------------------|
| Hex | Strings | File Metadata | Results | Message | Indexed Text | Media | Other Occurrences |
|-----|---------|---------------|---------|---------|--------------|-------|-------------------|

Matches on page: - of - Match < > Page: 1 of 1 Page < > Text Source: File Text

```

[Secret Project]

revised_points.ppt
This file is one of Gordons (http://digitalcorpora.org/corpora/gordons)
The first page is added by NIST CFS&DS project.
All following pages have no connection with to the scenario.

IREAP

+
Institute for Research in
Electronics & Applied Physics
University of Maryland, College Park, MD
NIST Research on the University of Maryland Electron Ring (UMER)
Research sponsored by US Department of Energy
Rami A. Kishket
on behalf of UMER collaboration

+

IREAP

+
We Thank:

University of Maryland Electron Ring (UMER) Team:
Rami A. Kishket

```

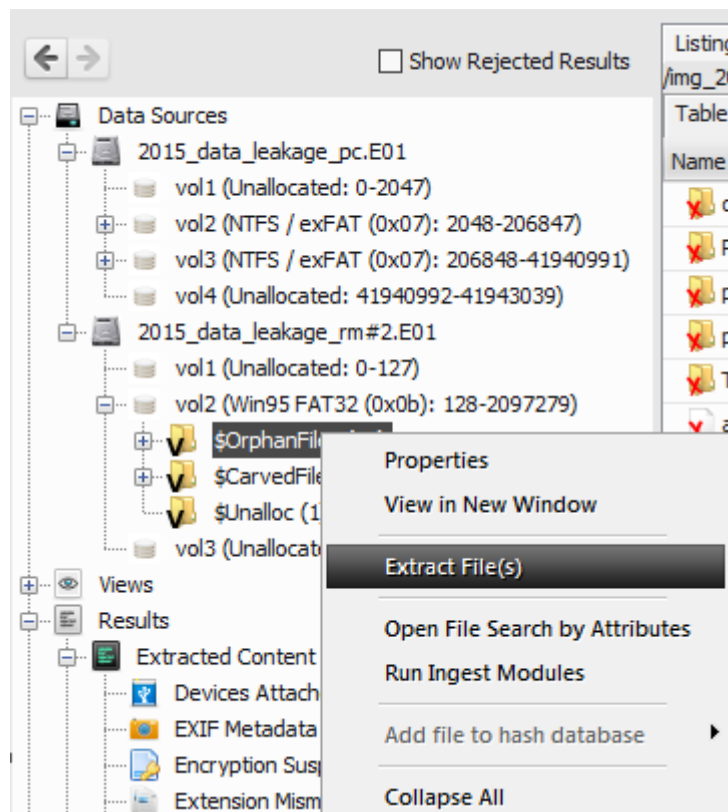
Kuvio 62 design

| | |
|-----------------------------|---|
| winter_whether_advisory.zip | [secret_project]_detailed_design.pptx |
| winter_storm.amr | [secret_project]_revised_points.ppt |
| new_years_day.jpg | (secret_project)_market_analysis.xlsx |
| super_bowl.avi | (secret_project)_market_shares.xls |
| my_favorite_movies.7z | (secret_project)_price_analysis_#1.xlsx |
| my_favorite_cars.db | (secret_project)_price_analysis_#2.xls |
| my_smartphone.png | [secret_project]_progress_#1.docx |
| my_friends.svg | [secret_project]_progress_#3.doc |
| a_gift_from_you.gif | [secret_project]_detailed_proposal.docx |
| landscape.png | [secret_project]_proposal.docx |
| diary_#1d.txt | [secret_project]_technical_review_#1.docx |
| diary_#1p.txt | [secret_project]_technical_review_#1.pptx |
| diary_#2d.txt | [secret_project]_technical_review_#2.docx |
| diary_#2p.txt | [secret_project]_technical_review_#2.ppt |
| diary_#3d.txt | [secret_project]_technical_review_#3.doc |

| | |
|---------------|--|
| diary_#3p.txt | [secret_project]_technical_review_#3.ppt |
|---------------|--|

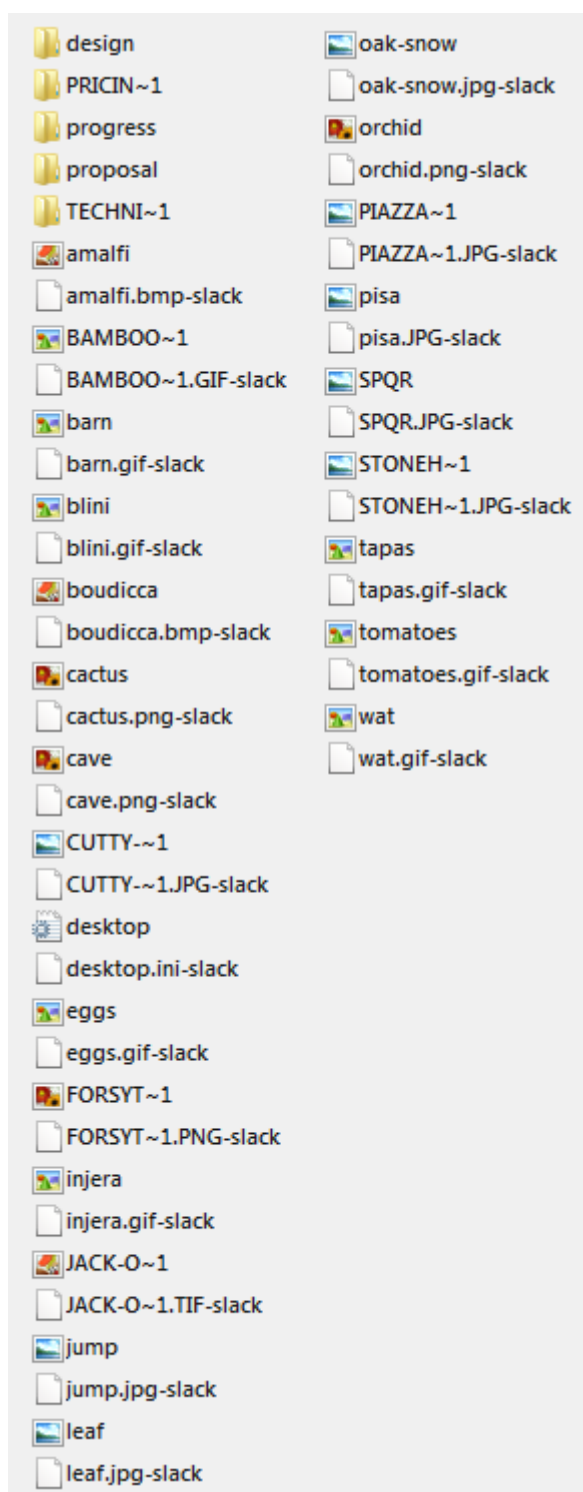
6.9 Tiedostojen palautus USB massamuistilta

Palautin tiedostot massamuistilta työpöydälle tarkasteltavaksi. (Kuvio 63)



Kuvio 63 Export massamuisti

Kaikki tiedostot näyttivät asiallisilta ja normaaleilta (Kuvio 64), kunnes testasin avata tiedostoja ja ne eivät toimineet. Testasin edellisessä kohdassa tehtyä taulukkoa ja muutin tiedostotyyppin oikeaksi. (Kuvio 65). Iaman Informant oli selvästi yrittänyt vuotaa yrityksen informaatiota.



Kuvio 64 exportatut tiedostot

a_gift_from_you - Saved to this PC

Layout References Mailings Review View Help Tell me what you want to do

Font Paragraph Styles

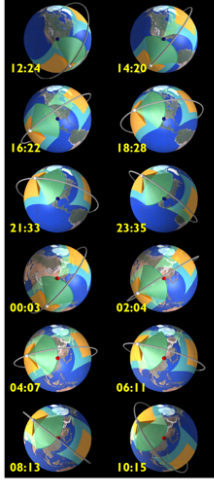
[Secret Project]

Detailed Proposal.docx

This file is one of Govdocs (<http://digitalcorporagovdocs>)
 The first page is added by NIST CEReDS project.
 All following pages have no connection with to the scenario.

INCOMPLETE ROUGH DRAFT

Composition of the Atmosphere from Mid-Earth Orbit (CAMEO)



CAMEO is a future mission concept submitted May 2005 to the U.S. National Research Council Decadal Survey on *Earth Science and Applications from Space*.

This update of CAMEO merges the Atmospheric Remote-sensing and Imaging Emission Spectrometer (ARIES) concept also submitted May 2005 to the Decadal Survey.

by

Joe Waters, Mouatda Chahine, Nathaniel Livesey, Thomas Pagano, Michelle Santee, Herman Adams, Paul Stek, Qianli Li, Duane Waliser, Richard Codefield, Annmarie Eldering, Eric Fetzer, Evie Fishbein, Michael Quam, Frederick Uson, Jonathan Jiang, Bjorn Lambrigsten, Sung-Yung Lee, Gloria Manney, Edward Olsen, William Read, Dong Wu

NASA Jet Propulsion Laboratory, California Institute of Technology, USA

Pieternel Levelt, Hennie Kelder, Bert van den Oord, Pippin Veldkin, Royal Netherlands Meteorological Institute, The Netherlands

Ike Aben and Anri Selig National Institute for Space Research, The Netherlands

Micha Goldberg and Chris Burnet NOAA National Environmental Satellite, Data, and Information Service, USA

John Le Marshall NOAA/NASA-DoD Joint Center for Satellite Data Assimilation, USA

Bob Atlas NOAA Atlantic Oceanography and Meteorological Laboratory, USA

Joel Susskind NASA Goddard Space Flight Center, USA

Laurie Strong and Wallace McMillan University of Maryland Baltimore County, USA

Bob Harwood and Hugh Pumphrey The University of Edinburgh, Scotland

CAMEO's overlapping coverage on successive orbits gives an unprecedented combination of temporal, vertical, and horizontal resolution, and global coverage needed for progress in atmospheric science and applications. Orange shows the ARIES and TROP instrument swaths; red shows the SAGE instrument swath. Yellow numbers are universal times of successive measurements over Houston (blue dot) and Beijing (red dot) for this simulated ~24-hour measurement period. Note that the illustration switches from western hemisphere to eastern

Kuvio 65 vuodettu dokumentti

7 Anti-forensiikka

7.1 Muutettuja rekisteriavaimia 23-25.3.2015

Rekisteriavaimia oltiin menty poistamaan (Kuvio 66)

| | | | | |
|---|-----------------------------------|---|-----|---------------------|
| ✖ | iCloudServices.PushService.1 | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.SyndNotifyIcon.1 | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.SyndNotifyIcon | 0 | 2 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.PushService | 0 | 2 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.AccountInfo.1 | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.AccountInfo | 0 | 2 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.ProxyInfo.1 | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.ProxyInfo | 0 | 2 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.NCAccount.1 | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | iCloudServices.NCAccount | 0 | 2 | 2015-03-25 15.19.06 |
| | AppID | 0 | 414 | 2015-03-25 15.19.06 |
| ✖ | ShellStreams.ShellStreamsView.1 | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | ShellStreams.ShellStreamsView | 0 | 2 | 2015-03-25 15.19.06 |
| ✖ | ShellStreams.ShellStreamsFolder.1 | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | ShellStreams.ShellStreamsFolder | 0 | 2 | 2015-03-25 15.19.06 |
| ✖ | Apple.DAV.Addin | 0 | 1 | 2015-03-25 15.19.06 |
| ✖ | cdaunch | 0 | 1 | 2015-03-25 15.18.37 |







Kuvio 66 poistettuja rekisteriavaimia

7.2 Forensiikka työtä vaikeuttavia toimenpiteitä

Herra Informant käytti anti-forensiikka työkaluja, joilla yritti tuhota forensiikka työt. Hän googlettel i eraseria ja ccleaneria, jotka asensi, käynnisti ja ajoi. Hän kirjautui ulos Google Drivestä ja poisti outlookista muutamia sähköposteja. Valitettavasti herra Informant ei tietänyt että kertaalleen tai edes 20 kertaan alustaminen tai datan poistaminen ei poista kokonaan dataa. Eraser löytyi koneelta asennettuna (Kuvio 67) ja ccleaner exe myös (Kuvio 68)

| img_2015_data_leakage_pc.E01\vol_03\Program Files\Eraser | | | | | | | | | | | | 17 Results |
|--|-------------------------|-------------------------|-------------------------|--------------------------|---------|-----------|-------------|------------|--------|---------|------------|------------|
| Table | Thumbnail | | | | | | | | | | | |
| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dr) | Flags(Meta) | Mode | UserID | GroupID | Meta Addr. | |
| [current folder] | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 56 | Allocated | Allocated | d-wx-wx-wx | 0 | 0 | 75197 | |
| [parent folder] | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2009-07-14 06:20:08 EEST | 192 | Allocated | Allocated | d-wx-wx-wx | 0 | 0 | 60 | |
| en | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 56 | Allocated | Allocated | d-wx-wx-wx | 0 | 0 | 75212 | |
| Plugins | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 56 | Allocated | Allocated | d-wx-wx-wx | 0 | 0 | 75204 | |
| algibnet2.dll | 2015-01-13 00:56:28 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:28 EET | 998472 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75199 | |
| BeveLine.dll | 2015-01-13 00:56:28 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:28 EET | 15432 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75201 | |
| CommonLibrary.dll | 2015-01-13 00:56:28 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:28 EET | 815688 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75203 | |
| DragDropLib.dll | 2015-01-13 00:56:28 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:28 EET | 41032 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75206 | |
| Eraser Documentation.pdf | 2015-01-13 00:54:48 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:54:48 EET | 606858 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75211 | |
| Eraser.exe | 2015-01-13 00:56:36 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:36 EET | 1085512 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75214 | |
| Eraser.Manager.dll | 2015-01-13 00:56:28 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:28 EET | 56904 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75215 | |
| Eraser.Plugins.dll | 2015-01-13 00:56:30 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:30 EET | 55368 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75217 | |
| Eraser.Shell.dll | 2015-01-13 00:56:34 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:34 EET | 209992 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75218 | |
| Eraser.Util.dll | 2015-01-13 00:56:30 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:30 EET | 111688 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75219 | |
| Eraser.Util.Native.dll | 2015-01-13 00:56:34 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:34 EET | 257096 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75221 | |
| Microsoft.Runtime.Hosting.dll | 2015-01-13 00:56:30 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:30 EET | 27720 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75229 | |
| TaskDialog.dll | 2015-01-13 00:56:30 EET | 2015-03-25 16:57:31 EET | 2015-03-25 16:57:31 EET | 2015-01-13 00:56:30 EET | 27208 | Allocated | Allocated | rwxrwxrwx | 0 | 0 | 75231 | |

Kuvio 67 eraser

| img_2015_data_leakage_pc.E01/vol_v03/Program Files/CCleaner | | | | | | | | | | | | 6 Results | |
|--|-----------|-------------------------|-------------------------|-------------------------|--------------------------|---------|-------------|-------------|------------|--------|---------|------------|-------|
| Table | Thumbnail | | | | | | | | | | | | |
| Name | | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID | Meta Addr. | Attr. |
|  [current folder] | | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2015-03-25 16:58:34 EET | 48 | Unallocated | Unallocated | drwxrwxrwx | 0 | 0 | 75246 | 144- |
|  [parent folder] | | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2009-07-14 06:20:08 EEST | 192 | Unallocated | Allocated | d-wx-wx-wx | 0 | 0 | 60 | 144- |
|  Lang | | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2015-03-25 17:18:37 EET | 2015-03-25 16:58:35 EET | 48 | Unallocated | Unallocated | drwxrwxrwx | 0 | 0 | 75251 | 144- |
|  CCleaner.exe | | 2015-03-13 13:10:26 EET | 2015-03-25 17:18:36 EET | 2015-03-25 16:58:35 EET | 2015-03-13 13:10:26 EET | 5529680 | Unallocated | Unallocated | rwxrwxrwx | 0 | 0 | 75248 | 128- |
|  CCleaner64.exe | | 2015-03-13 13:10:26 EET | 2015-03-25 17:18:36 EET | 2015-03-25 16:58:35 EET | 2015-03-13 13:10:26 EET | 7451928 | Unallocated | Unallocated | rwxrwxrwx | 0 | 0 | 75250 | 128- |
|  uninst.exe | | 2015-03-13 15:55:38 EET | 2015-03-25 17:18:36 EET | 2015-03-25 16:58:35 EET | 2015-03-13 15:55:38 EET | 154384 | Unallocated | Unallocated | rwxrwxrwx | 0 | 0 | 75307 | 128- |

Kuvio 68 ccleaner exe

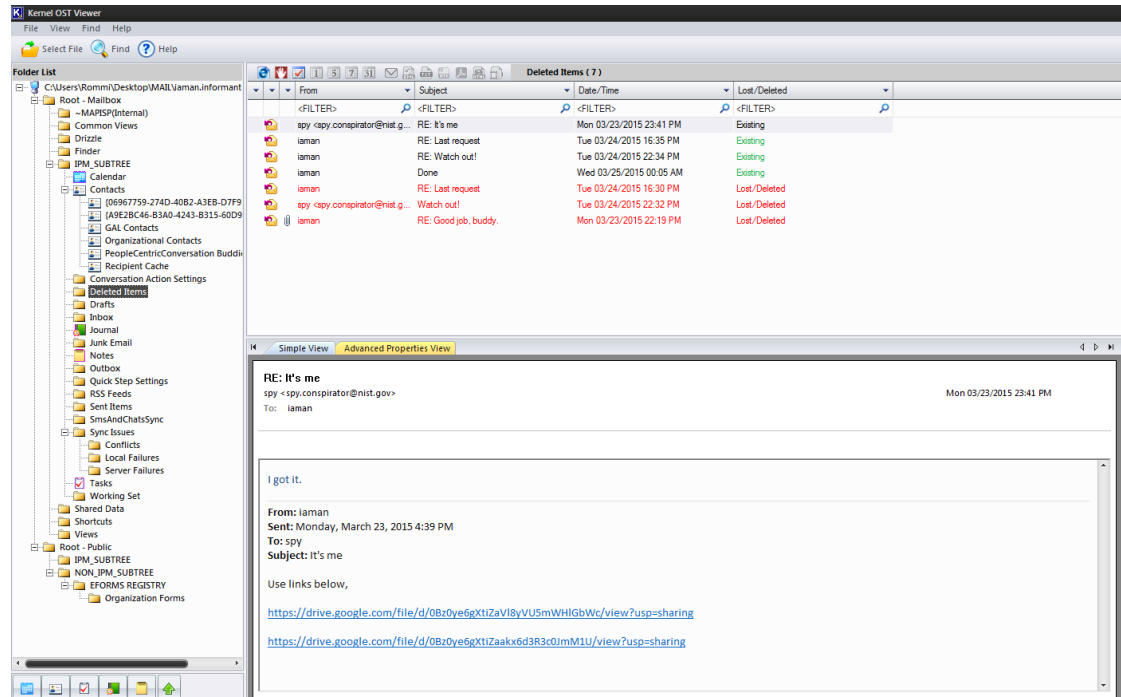
7.3 Oleellisia asioita tutkimuksessa

Löysin tutkiessani AppDataa Microsoft Outlook kansion alta laman Informantin outlook sähköposti ost tiedoston, mikä tarkoitti sitä että hänen lähettämäänsä sähköposteja pääsisi lukemaan. (Kuvio 69)

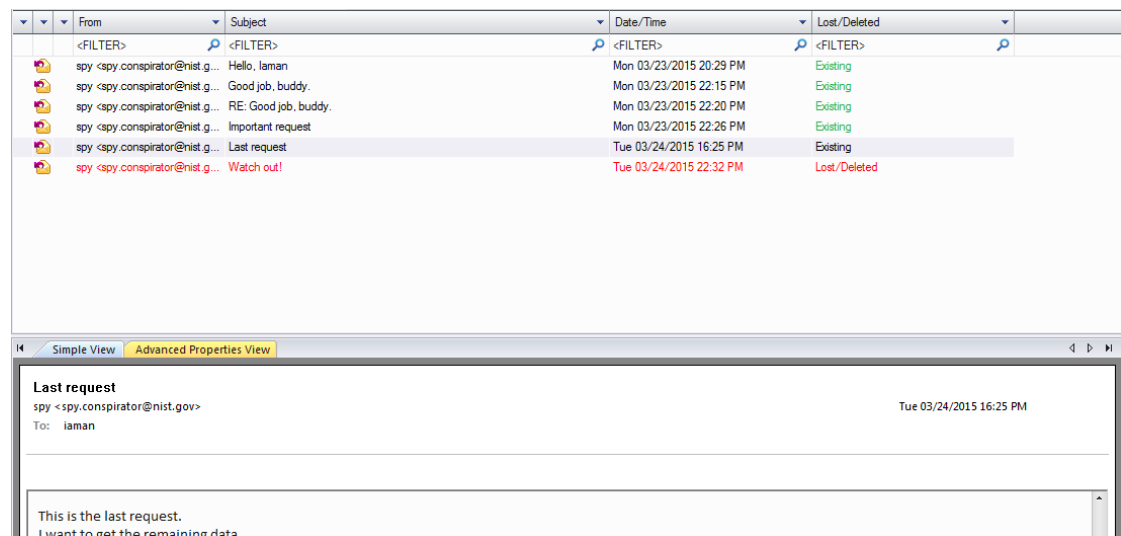
| /img_2015_data_leakage_pc.E01/vol3/Users/Informant/AppData/Local/Microsoft/Outlook | | | | | | | | | | | |
|--|-----------|-------------------------|-------------------------|-------------------------|-------------------------|----------|-------------|-------------|------------|--------|---------|
| Name | Thumbnail | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | UserID | GroupID |
| [current folder] | | 2015-03-25 17:11:47 EET | 2015-03-25 17:11:47 EET | 2015-03-25 17:11:47 EET | 2015-03-22 17:46:02 EET | 56 | Allocated | Allocated | drwxrwxrwx | | |
| [parent folder] | | 2015-03-23 19:29:57 EET | 2015-03-23 19:29:57 EET | 2015-03-23 19:29:57 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | drwxrwxrwx | | |
| Offline Address Books | | 2015-03-22 17:50:21 EET | 2015-03-22 17:50:21 EET | 2015-03-22 17:50:21 EET | 2015-03-22 17:50:21 EET | 312 | Allocated | Allocated | drwxrwxrwx | | |
| RoamCache | | 2015-03-23 21:29:29 EET | 2015-03-23 21:29:29 EET | 2015-03-23 21:29:29 EET | 2015-03-22 17:48:37 EET | 56 | Allocated | Allocated | drwxrwxrwx | | |
| fc39fbc85bcb43816b40b7d4c72f22 - Autodiscover.xml | | 2015-03-25 16:41:36 EET | 2015-03-25 16:41:36 EET | 2015-03-22 17:48:05 EET | 2015-03-22 17:48:05 EET | 10074 | Allocated | Allocated | rw-rw-rw-x | | |
| laman.informant@nist.gov.ost | | 2015-03-25 17:11:47 EET | 2015-03-25 17:11:47 EET | 2015-03-22 17:48:21 EET | 2015-03-22 17:48:21 EET | 16818176 | Allocated | Allocated | rwxrwxrwx | | |
| mapisvc.inf | | | | 03-25 16:41:03 EET | 2015-03-24 15:25:20 EET | 1324 | Allocated | Allocated | rwxrwxrwx | | |
| ~laman.informant@nist.gov.ost.tmp | | | | 03-25 16:41:04 EET | 2015-03-25 16:41:04 EET | 131072 | Unallocated | Unallocated | rw-rw-rw-x | | |
| ~laman.informant@nist.gov.ost.tmp | | | | 00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | | ----- | | |

Kuvio 69 export .ost

Käynnistin Kernel OST Viewerin ja avasin exportatun .ost tiedoston. laman Informant ei ollut lähettänyt paljon viestejä, mutta kaikki keskustelut käytiin spy.conspirator@nist.gov kanssa (Kuvio 71). Keskusteluista sai selville että spy antoi ohjeita laman Informantille kuinka datan toimituksessa toimitaan. (Kuvio 70) Tämä oli viimeinen tikki arkkuun, joka varmensi laman Informantin tietovuoto rikoksen.



Kuvio 70 chat 1



Kuvio 71 chat 2

Myös aijemmin dokumentaatioissa todetut google haut olivat hieman epäilyttäviä, varsinkin hakujen välinen aika ja hakujen yhtäläisyys (Kuvio 72)

```
.#q=system+cleaner&hl=en&start=10
.#q=information+leakage+cases&hl=en
.#q=how+to+recover+data&hl=en&start=20
.#q=how+to+recover+data&hl=en&start=10
.#hl=en&q=system+cleaner
.#hl=en&q=intellectual+property+theft
.#hl=en&q=how+to+recover+data
.#hl=en&q=how+to+leak+a+secret
.#hl=en&q=how+to+delete+data
.#hl=en&q=digital+forensics
.#hl=en&q=data+recovery+tools
.#hl=en&q=data+recovery+tools
.#hl=en&q=cloud+storage
.#hl=en&q=anti-forensics
```

Kuvio 72 epäilyttävät haut

laman informant oli kirjoittanut myös 24.03.2015 sticky noten missä kerrotaan että Huomenna..... Kaikki on ihan OK..... (Kuvio 73) Viesti on erittäin hämärä, laman Informantin käytöksen takia, viesti joko viittaa kiinni jäämiseen tai haluun toteuttaa itsemurha.

/img_2015_data_leakage_pc.E01/vol_vol3/Users/Informant/AppData/Roaming/Microsoft/Sticky Notes 3 Results

| Name | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Mode | Use |
|------------------|-------------------------|-------------------------|-------------------------|-------------------------|------|------------|-------------|------------|-----|
| [current folder] | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 272 | Allocated | Allocated | drwxrwxrwx | 0 |
| [parent folder] | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 2015-03-22 16:34:41 EET | 56 | Allocated | Allocated | drwxrwxrwx | 0 |
| StickyNotes.snt | 2015-03-24 20:31:59 EET | 2015-03-24 20:31:59 EET | 2015-03-24 20:30:09 EET | 2015-03-24 20:30:09 EET | 4096 | Allocated | Allocated | rwxrwxrwx | 0 |

Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences

Page: 1 of 1 Page Go to Page: Script: Latin - Basic

```
Root Entry
Version
Metafile
ccbb72fb-d253-11e4-b
ccbb72fb-d253-11e4-b
{\ttf\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\fsa0
rsat0 Segoe Print;\f1\fnil Segoe Print;}}
{\*\generator Msoftedit 9.41.21.2510;}
\viewkind4\uc1\pard\tx360\tx720\tx1080\tx1440\tx1800\tx2160\tx2520\tx2880\tx3240\tx3600\tx3960\tx4320\tx4680\tx5040\tx5400\tx5760\tx6120\tx6480\tx6
Tomorrow...\par
\par
Everything will be OK...\par
\par
\lang9\fi\par
Tomorrow...
Everything will be OK...
```

Kuvio 73 sticky note

7.4 Todisteet tietovuodosta

Sain mielestäni tarpeeksi todistusaineistoa tietovuodosta, sillä minulla on todisteet kaikista 22-25.03.2015 käydyistä tapahtumista. Tapahtumiin kuuluu:

- käydyt keskustelut
- google hauist

- käydyt sivut
- asennetut ohjelmat
- jaetut tiedostot
- poistetut tiedostot
- rekisterit
- käyttäjä joka viimeksi kirjautunut ja viimeks poistunut
- siirretyt tiedostot
- uudelleen nimetyt tiedostot

Saamieni todisteiden pohjalta laman Informant voidaan tuomita oikeudessa vankilaan. Kerätty todistusaineisto on paljon ja se kattaa yritys vakoilu, vaitiolovelvollisuuden rikkomiset, jne.

7.5 Aikajana tapahtumista

| 22.03.2015 | 23.03.2015 | 24.03.2015 | 25.03.2015 |
|----------------------------|-------------------------------------|---------------------------------|------------------------------------|
| Käyttöjärjestelmän asennus | Epämääräisten asioiden googlaaminen | Tiedostojen nimien muuttaminen | Antiforensiikka työkalujen asennus |
| Ohjelmiston asennus | Spyn kanssa kommunikointi | Tikulle tiedostojen kopioiminen | Spostien poistaminen |
| | Google Driven asentaminen | | |
| | Google Driveen Uploadaaminen | | |

8 Pohdinta

Tehtävä oli suoraan loistava! Tällä kurssilla ja työn aikana opin paljon uusia asioita, työkaluja ja jäin janoamaan lisää metsästettävää rekistereistä ja koneelta. Tehtävä tuntui aluksi hirveän laajalta, mutta asennusten jälkeen homma ei ollutkaan niin kauhean massiivinen. Työ oli todella hauska, mutta aivan hirveän raskas dokumentoida kuvien takia. Työhön itsessään meni joku suurin piirtein 10 tuntia ja dokumentaatioon ~10h myös varmaan. Työssä haastavinta oli ehkä oppia registry explorerin ja oikeiden rekisteri hivejen käyttäminen. Paljon aikaa meni hukkaan kun kahlasin hamistorakenteissa, enkä tajunnut että ohjelmassa on bookmarkseja, sekä haku työkalu niiden lisäksi. Tajusin asian liian myöhään että siitä olisi ollut ajallisesti mitään hyötyä. Työ vaati todella paljon googlettamista, sillä en ulkomuistista muista missä mikäkin asia sijaitsee, joten google toimi hyvänä ystävänä. Olisi ollut mielenkiintoista koostaa sekuntin tarkkuudella kaikki tapahtumat, mutta oma osaaminen tällä hetkellä ei siihen riittänyt. Aikajana on toteutettu aika päällisin puolin päivä kerrallaan, aikaa määrittämättä. Lisää tälläisiä tehtäviä!

9 Lähteet

Brian Conner, Autopsy n.d. <http://www.sleuthkit.org/autopsy/>

Kernel Data Recovery, Kernel OST Viewer n.d.

<https://www.nucleustechnologies.com/ost-viewer.html>

Eric Zimmerman Github, n.d. <https://ericzimmerman.github.io/>

Marko Vatanen Digital Forensics -harjoitus 16.01.2017

<https://optima.jamk.fi/learning/id2/bin/user?rand=51112>

Marko Vatanen Digital Forensics Materiaali n.d.

<https://optima.jamk.fi/learning/id2/bin/user?rand=51112>

user40980 Calculating disk capacity and max data transfer rate of a hard drive

<https://softwareengineering.stackexchange.com/questions/278802/calculating-disk-capacity-and-max-data-transfer-rate-of-a-hard-drive>

Wikipedia Windows Registry n.d. https://en.wikipedia.org/wiki/Windows_Registry

Wikipedia Shadow Copy n.d. https://en.wikipedia.org/wiki/Shadow_Copy