

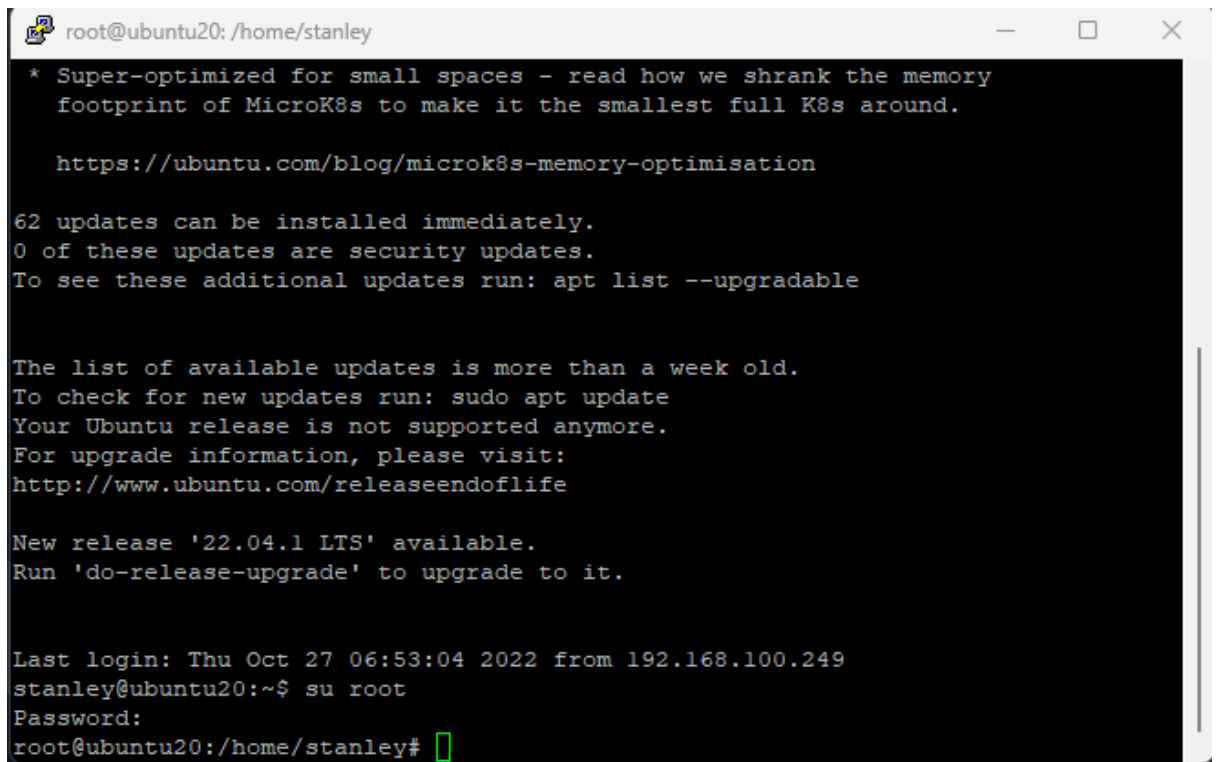
WRITE-UPS LKSN DAY 3

TEAM KALIMANTAN SELATAN

AHMAD RYAN FAIZAL
A. ATHOILLAH

Patching

Diberikan VM day 2 kemarin untuk kita patching di day 3 kali ini. Jadi tentu saja hal yang pertama kali saya lakukan adalah login ke VM-nya menggunakan SSH untuk mempermudah patching.



```
root@ubuntu20: /home/stanley

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

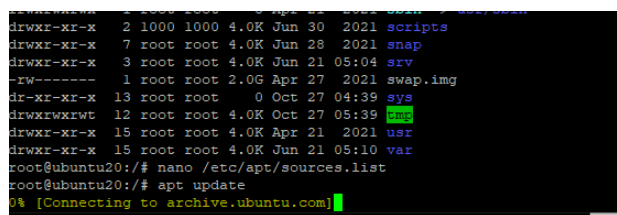
62 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Oct 27 06:53:04 2022 from 192.168.100.249
stanley@ubuntu20:~$ su root
Password:
root@ubuntu20:/home/stanley#
```

Setelah itu kami langsung saja melakukan update pada vmnya agar mendapatkan patch atau juga bug fix dari versi yang lama.



```
dpkg-query -f='${Package} ${Version} ${Architecture} ${InstallSize} ${Date} ${Source} ${Description}\n' -W
drwxr-xr-x 2 1000 1000 4.0K Jun 30 2021 scripts
drwxr-xr-x 7 root root 4.0K Jun 28 2021 snap
drwxr-xr-x 3 root root 4.0K Jun 21 05:04 srv
-rw-r--r-- 1 root root 2.0G Apr 27 2021 swap.img
dr-xr-xr-x 13 root root 0 Oct 27 04:39 sys
drwxrwxrwt 12 root root 4.0K Oct 27 05:39 tmp
drwxr-xr-x 15 root root 4.0K Apr 21 2021 usr
drwxr-xr-x 15 root root 4.0K Jun 21 05:10 var
root@ubuntu20:/# nano /etc/apt/sources.list
root@ubuntu20:/# apt update
0% [Connecting to archive.ubuntu.com]
```

Setelah update selesai, kami melakukan pengecekan menggunakan utility iptables yang sudah ada terlihat ada port yang diperbolehkan dan yang tidak diperbolehkan (reject)

```

root@ubuntu20:/var/www/html# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:ssh
ACCEPT     tcp  --  192.168.1.128          anywhere             tcp dpt:ssh
REJECT     tcp  --  anywhere              anywhere             tcp dpt:2409 reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@ubuntu20:/var/www/html#

```

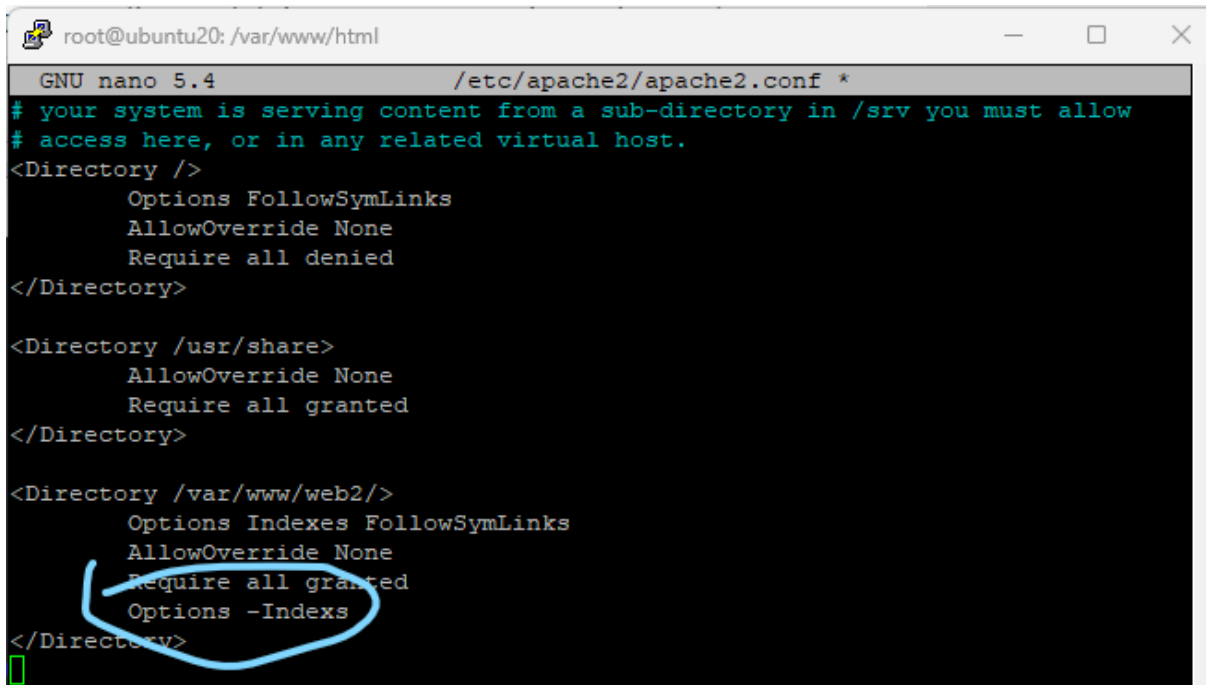
dan kami juga melakukan pengecekan pada port yang terbuka dengan utility yang sudah tersedia juga dengan perintah `isof -nP -iTCP -sTCP:LISTEN`

```

root@ubuntu20:/var/www/html# isof -nP -iTCP -sTCP:LISTEN
COMMAND  PID    USER      FD  TYPE  DEVICE  SIZE/OFF  NODE  NAME
systemd-r 655    systemd-r 13u  IPv4  19546   0t0      TCP  127.0.0.53:53 (LISTEN)
vsftpd    693    root      3u   IPv6  19877   0t0      TCP  *:21 (LISTEN)
sshd      759    root      3u   IPv4  20107   0t0      TCP  *:22 (LISTEN)
sshd      759    root      4u   IPv6  20127   0t0      TCP  *:22 (LISTEN)
mysqld    843    mysql     22u  IPv4  21569   0t0      TCP  127.0.0.1:33060 (LISTEN)
mysqld    843    mysql     34u  IPv4  21647   0t0      TCP  127.0.0.1:3306 (LISTEN)
dnsmasq   4040   lxd       9u   IPv4  30964   0t0      TCP  10.214.70.1:53 (LISTEN)
dnsmasq   4040   lxd      11u  IPv6  30966   0t0      TCP  [fe80::e0d2:d6ff:fe8f:7672]:53 (LISTEN)
dnsmasq   4040   lxd      13u  IPv6  30968   0t0      TCP  [fd42:51ce:6f37:44c9::1]:53 (LISTEN)
root@ubuntu20:/var/www/html#

```

Kami juga merubah konfigurasi terhadap apache default dengan melakukan perubahan pada `apache.conf` kami menambahkan script untuk mematikan listing directory dan versi dari apache tersebut untuk mengurangi info yang didapatkan dari segi server.



```

GNU nano 5.4 /etc/apache2/apache2.conf *
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/web2/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
    Options -Indexes
</Directory>

```

```
GNU nano 5.4 /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

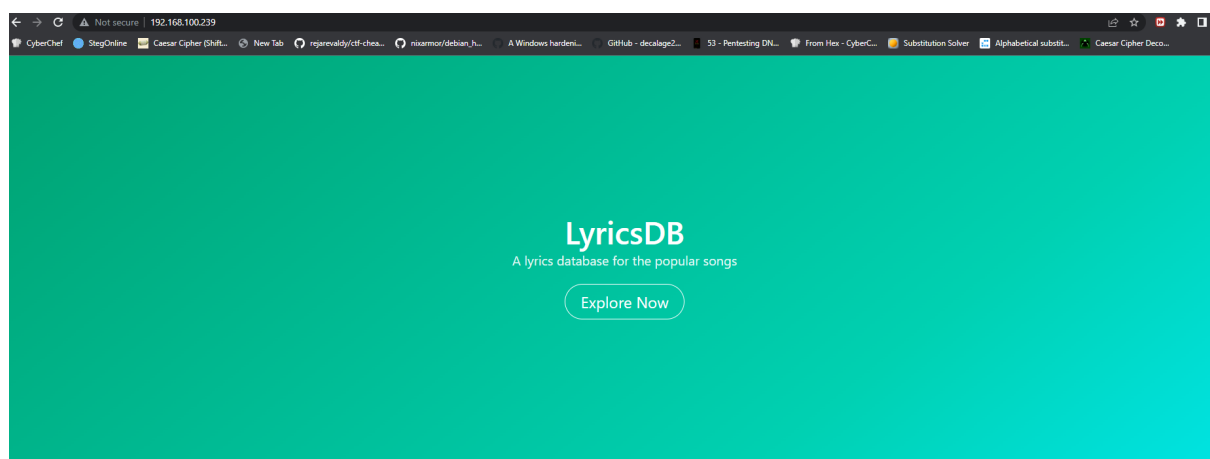
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/web2

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log

    [ Read 31 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Setelah melakukan konfigurasi tersebut jadilah seperti ini



Kami juga mengidentifikasi sebuah file yang rentan untuk diretas seperti dibawah ini yang permissionnya lemah kami melakukan perubahan hak akses dan hak permission

```

root@ubuntu20:/var/www/html# ls -lah
total 36K
drwxr-xr-x 3 root    root    4.0K Oct 27 09:46 .
drwxr-xr-x 4 root    root    4.0K Oct 25 00:09 ..
-rwxr-xr-x 1 root    root    522 Apr 29 2021 .backup_config.php
-rw-r--r-- 1 root    root    1.0K Oct 27 09:46 ..backup_config.php.swp
-rw-r--r-- 1 www-data www-data 12K Jun 30 2021 index.html
-rw-r--r-- 1 www-data www-data 43 Oct 25 00:10 robots.txt
drw----- 2 www-data www-data 4.0K Jun 21 16:28 very_secret_dir
root@ubuntu20:/var/www/html# chmod 600 .backup_config.php
root@ubuntu20:/var/www/html# chown www-data:www-data .backup_config.php
root@ubuntu20:/var/www/html# ls -lah
total 36K
drwxr-xr-x 3 root    root    4.0K Oct 27 09:46 .
drwxr-xr-x 4 root    root    4.0K Oct 25 00:09 ..
-rw----- 1 www-data www-data 522 Apr 29 2021 .backup_config.php
-rw-r--r-- 1 root    root    1.0K Oct 27 09:46 ..backup_config.php.swp
-rw-r--r-- 1 www-data www-data 12K Jun 30 2021 index.html
-rw-r--r-- 1 www-data www-data 43 Oct 25 00:10 robots.txt
drw----- 2 www-data www-data 4.0K Jun 21 16:28 very_secret_dir

```

Kami melihat sebuah log mencurigakan dari service FTP seperti yang sudah kami screenshot dibawah ini

```

Tue Oct 25 00:08:37 2022 [pid 3796] CONNECT: Client "::ffff:192.168.5.200"
Tue Oct 25 00:08:42 2022 [pid 3795] [ftp] OK LOGIN: Client "::ffff:192.168.5.200", anon password "?"
Tue Oct 25 00:09:26 2022 [pid 3797] [ftp] OK DOWNLOAD: Client "::ffff:192.168.5.200", "/note.txt", 192 bytes, 54.32Kbyte/sec
Tue Oct 25 00:10:54 2022 [pid 3863] CONNECT: Client "::ffff:192.168.5.200"
Tue Oct 25 00:11:21 2022 [pid 3862] [sysadm] FAIL LOGIN: Client "::ffff:192.168.5.200"
Tue Oct 25 00:11:29 2022 [pid 3866] CONNECT: Client "::ffff:192.168.5.200"
Tue Oct 25 00:11:33 2022 [pid 3865] [sysadm] OK LOGIN: Client "::ffff:192.168.5.200"
Tue Oct 25 00:40:36 2022 [pid 4099] CONNECT: Client "::ffff:192.168.5.200"
Tue Oct 25 00:41:00 2022 [pid 4098] [sysadm] OK LOGIN: Client "::ffff:192.168.5.200"
Tue Oct 25 00:41:31 2022 [pid 4104] CONNECT: Client "::ffff:192.168.5.200"
Tue Oct 25 00:41:35 2022 [pid 4103] [ftp] OK LOGIN: Client "::ffff:192.168.5.200", anon password "?"
Tue Oct 25 00:41:38 2022 [pid 4105] [ftp] OK DOWNLOAD: Client "::ffff:192.168.5.200", "/note.txt", 192 bytes, 118.15Kbyte/sec
Tue Oct 25 00:41:43 2022 [pid 4107] CONNECT: Client "::ffff:192.168.5.200"
Tue Oct 25 00:41:51 2022 [pid 4106] [sysadm] OK LOGIN: Client "::ffff:192.168.5.200"
Tue Oct 25 00:41:57 2022 [pid 4108] [sysadm] OK DOWNLOAD: Client "::ffff:192.168.5.200", "/backup.conf.enc", 299 bytes, 39.64Kbyte/sec
root@ubuntu20:/var/log#

```

Setelah melihat log diatas kami menemukan kerentanan di dalam service FTP karena membolehkan user anonymous dan akses ssh menggunakan ftp

```

GNU nano 5.4 /etc/vsftpd.conf *
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
anon_root=/var/ftp/pub

```

Memory forensic Bully

Challenge

2 Solves

×

1. Ketagihan

100

Laman file: <https://drive.google.com/file/d/1RQ-IT-yW-iCTPgX8EfVOflGfNIQHU3X/view?usp=sharing>

Password file: peserta_LKSN_terlalu_GG_dan_OP_2k22!

Bagian Pertama

Awal Deskripsi Kasus:

Bobby, merupakan seorang anak SMA yang sangat nakal. Ia pernah masuk ke dalam penjara remaja sejak SMP karena kelakuannya yang suka menjahili temannya hingga berlebihan. Kini, Bobby berubah lagi hingga membuat banyak temannya merasa kesal dengannya hingga dipanggil polisi daerah. Bobby gemar menutupi jejak aksinya dan sangat terencana, oleh karena itu polisi daerah diberikan penugasan untuk mengecek HP Bobby jika ada keanehan atau kekeliruan di dalamnya. Anda, sebagai tim Digital Forensik yang dapat diandalkan diminta untuk melakukan analisa dari hasil akuisisi sebuah **Android Image Phone**.

Pertanyaan:

Apa nama aplikasi *browser* yang digunakan oleh tersangka?
(nama *Android Package Name*)

Format: com.apapunini.mbahgugel

Flag

Submit

Diberikan sebuah memory forensic yang dimana memory forensic tersebut akan berhubungan dengan soal soal berikut nya, Pertama kami menggunakan tool Aleapp([abrignoni/ALEAPP: Android Logs Events And Protobuf Parser \(github.com\)](https://github.com/abrignoni/ALEAPP)) untuk memforensic memory yang diberikan, berikut kami jabarkan cara penginstalannya

1. Mengunjungi link <https://github.com/abrignoni/ALEAPP>
2. Unduh requirements.txt
3. run command `python -m pip install -r requirements.txt`
4. Setelah itu unduh aleapp dengan wget ke <https://github.com/abrignoni/ALEAPP/archive/refs/heads/master.zip>
5. Extract master.zip

```

(kali@kali)-[~]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
ERROR: Invalid requirement: '<DOCTYPH.html>' (from line 8 of requirements.txt)

(kali@kali)-[~]
└─$ nano requirements.txt
└─$ nano requirements.txt
└─$ rm requirements.txt
└─$ cat requirements.txt
cat: requirements.txt: No such file or directory

(kali@kali)-[~]
└─$ nano requirements.txt
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Ignoring python-magic-bin: markers 'platform_system == "Windows"' don't match your environment
Ignoring python-magic-bin: markers 'platform_system == "Darwin"' don't match your environment
Requirement already satisfied: bcrypt==3.2.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (3.2.0)
Collecting BeautifulSoup4==4.8.2
  Downloading BeautifulSoup4-4.8.2-py3-none-any.whl (106 kB)
    100.9/106.9 kB 23.8 kB/s eta 0:00:00
Collecting blackboxprotobuf
  Downloading blackboxprotobuf-1.0.1.tar.gz (14 kB)
  Preparing metadata (setup.py) ... done
Collecting packaging-20.1
  Downloading packaging-20.1-py2.py3-none-any.whl (36 kB)
Collecting protobuf==3.10.0
  Downloading protobuf-3.10.0-py2.py3-none-any.whl (434 kB)
    434.9/434.9 kB 27.4 kB/s eta 0:00:00
Collecting PyCryptodome
  Downloading pycryptodome-3.15.0-cp35-abi3-manylinux2010_x86_64.whl (2.3 MB)
    2.3/2.3 MB 74.7 kB/s eta 0:00:00
Collecting PySimpleGUI==4.16.0
  Downloading PySimpleGUI-4.16.0-py3-none-any.whl (306 kB)
    306.2/306.2 kB 127.2 kB/s eta 0:00:00
Collecting simplekml
  Downloading simplekml-1.3.6.tar.gz (52 kB)
    53.0/53.0 kB 110.2 kB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Requirement already satisfied: wheel in /usr/lib/python3/dist-packages (from -r requirements.txt (line 9)) (0.37.1)
Requirement already satisfied: xmltodict in /usr/lib/python3/dist-packages (from -r requirements.txt (line 10)) (0.13.0)
Collecting filetype==1.0.8
  Downloading filetype-1.0.8-py2.py3-none-any.whl (16 kB)
Collecting python-magic==0.4.24
  Downloading python_magic-0.4.24-py2.py3-none-any.whl (12 kB)
Requirement already satisfied: pillow in /usr/lib/python3/dist-packages (from -r requirements.txt (line 15)) (9.2.0)
Requirement already satisfied: soupsieve>1.2 in /usr/lib/python3/dist-packages (from BeautifulSoup4==4.8.2->-r requirements.txt (line 2)) (2.3.2)

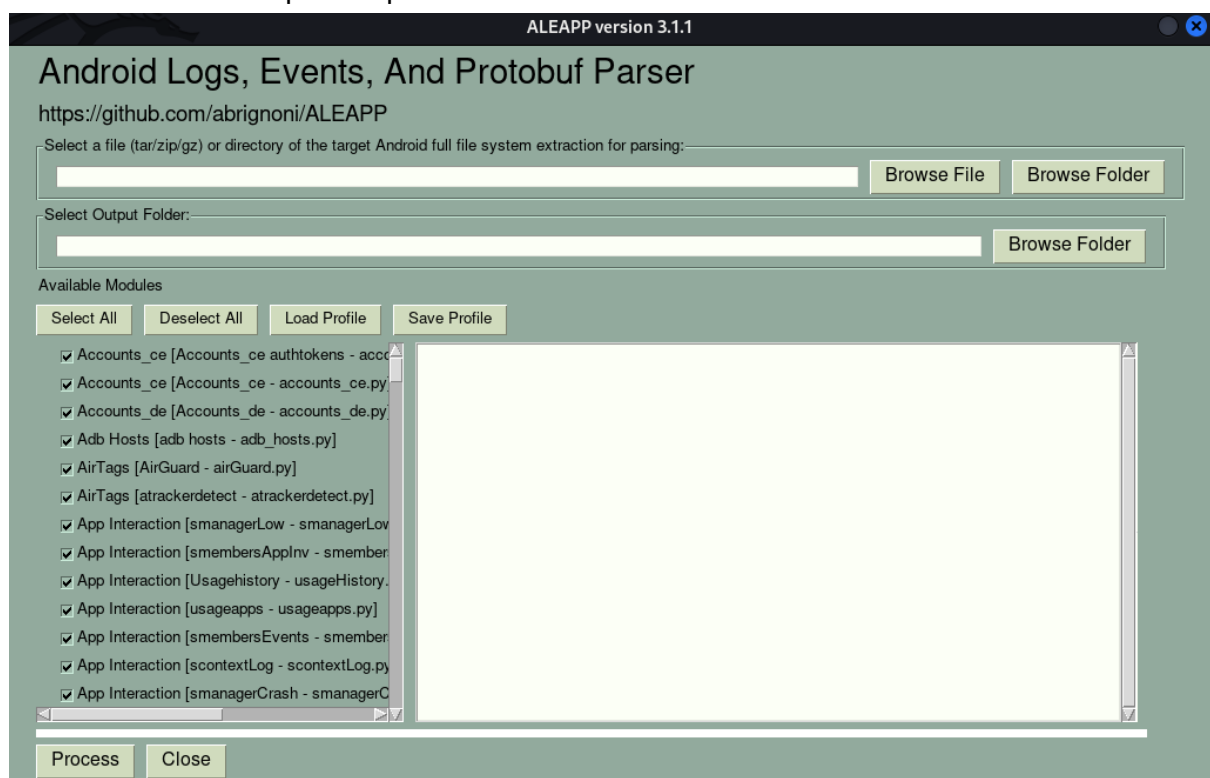
```

6.

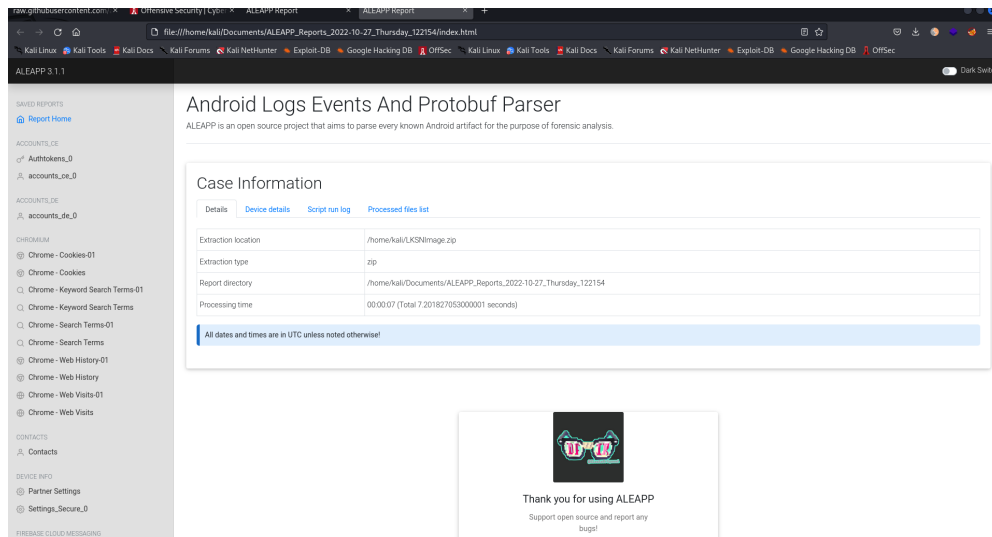
Cara running ALEAPP

1. Masuk ke folder Aleapp yg sudah di ekstrak
2. Jalankan perintah `$ python aleappGUI.py`

dan akan muncul tampilan seperti berikut



Kami memasukkan file memory yang sudah diberikan dan tools akan berjalan



Karena soal pertama meminta kami untuk mencari browser apa yang digunakan Bobby jadi kami melihat dibagian package apa saja yang di install bobby dan ditemukan lah browser yang dia gunakan

Bundle ID
com.android.chrome
com.android.vending
com.discord
com.google.android.apps.docs.editors.docs
com.google.android.keep
com.instagram.android
com.keramidas.TitaniumBackup
com.keramidas.TitaniumBackupAddon
Bundle ID

solution 1 (com.android.chrome)

2. Sumber Kenakalan

Challenge

1 Solves

×

2. Sumber Kenakalan

100

Bagian Kedua

Pihak kepolisian menerka sumber kenakalan remaja Bobby berasal dari kecanduan aplikasi ataupun dari lingkungan pertemanannya. Laman URL apa yang dikunjungi oleh Bobby yang pertama kali-nya selain Google ?

Format: <http://inihanyasebascontohsajaya.com>

<div> <div>🔍 Chrome - Search Terms</div> <div>📅 Chrome - Web History-01</div> <div>🌐 Chrome - Web History</div> <div>🌐 Chrome - Web Visits-01</div> <div>🌐 Chrome - Web Visits</div> <div>CONTACTS</div> <div>👤 Contacts</div> </div>	<div> <div>08/20/27</div> <div>gs_jcp=CHNtbzJpbGJlZ3d3dXdpelzKXwEAMyCAGAEIAEEDMgslABCBBCXAvxCDATIFCAAQgAyQyBgQAEIEMgJlABCBDFICAAQgAyQyBgQAEIEMgJlABCBAbDCLC04qAQsQmQgwE6BgAeEMQwAeEAGyAEIAELEDEOgcIABCXvxBDgQyABgQACDARB8g0gllnCvXvAUAB8D0ggIABgCXvCDAtKCAAGAQsQmQgwEQCjgHCAAGAQQOjKCAAGAQsQmQMQKQeEEEPYEAoFCBISATFQSPBNWlWmTdEqe5BKAaAcAGAAcUAG8GJBtXcJlUxJmUzBgBAKABApABAMABAg&scit=mobile-gws-wiz=seer</div> </div>	<div> <div>bully - Penelusuran Google</div> <div>Download Bully: Anniversary Edition (MOD, Unlimited Money) 1.0.0.18 APK for android</div> </div>	<div> <div>1</div> <div>0</div> <div>26</div> </div>
<div> <div>2022-10-26</div> <div>https://www.google.com/search?q=cara+meniadi+pembully+trend+2022&qg=cara+meniadi+pem&qgs=chrome.0.69</div> </div>	<div> <div>cara meniadi</div> </div>	<div> <div>1</div> <div>0</div> <div>27</div> </div>	

Challenge 0 Solves

Flag Submit

2022-10-26 08:20:59	account.kompas.com	AWSALB	sgWKElEwdy55aeclIW6toBhZ9IX9f+4dq5fJjsQaYdXkf2ofKniWI1H/aBOqZ7rCT5+S8Ub5/a+32LILqMcCBIrJ4K8iVKfd+Jvop+S9BiA3LxeJpGaVEWC
2022-10-26 08:20:59	account.kompas.com	AWSALBCORS	sgWKElEwdy55aeclIW6toBhZ9IX9f+4dq5fJjsQaYdXkf2ofKniWI1H/aBOqZ7rCT5+S8Ub5/a+32LILqMcCBIrJ4K8iVKfd+Jvop+S9BiA3LxeJpGaVEWC

**Solutions3(sgWKELEwdy55aecllW6ToBhZ9iXi9F+d4qb5FfjsQaYdXkf2ofKnIWI1H/aB0qZ7t
RCT5+S8Ub5/a+32LILqMccBIRj4K8iVKfd+Jvop+Sj9BiA3LxkeJpGaVEWC)**

4. Korek Menyala

Challenge 0 Solves

4. Korek Menyala
100

Bagian Keempat

Anda mengecek jika laman pencarian teratas yang dicari Bobby pada *browser*-nya mengindikasikan perilaku sosiopat. Apakah hasil pencarian **teratas** saat Bobby sedang menggunakan **search bar browser** -nya?

Format: ini hasil pencariannya guys pakai spasi

Flag Submit

Kami disuruh mengecek hasil pencarian teratas browser nya bobby yang mengindikasikan perilaku sosiopat

[illegible]

Solution4(cara menjadi pembully yang benar - Penelusuran Google)

5. Tertata rapi

Challenge 0 Solves X

5. Tertata Rapi

100

Bagian Kelima

Bobby ternyata menyimpan rencananya pada sebuah aplikasi *note-taking* khusus. Apa nama aplikasi yang digunakan penyerang untuk melakukan *note taking*? (nama *package name* Android-nya)

Format: com.lksn.menangsemua

Flag Submit

Kami disuruh menyelidiki nama aplikasi note-taking khusus yang digunakan bobby dengan format package nya

 Installed Apps (GMS)

com.google.android.keep

Solution5(com.google.android.keep)

6. Akal Licik Anak SMA

Challenge 0 Solves X

6. Akal Licik Anak SMA

100

Bagian Keenam

Bobby telah tertangkap basah oleh Anda karena Anda mengetahui bahwa dia telah menyusun rencana usilnya yang masih dalam aplikasi *note-taking*-nya. Siapakah nama dari korban pertama rencana jahatnya? (huruf kecil semua tanpa spasi)

Format: namabiassa

Flag Submit

Kami disuruh mencari korban pertama rencana jahat nya boby yang berada di dalam aplikasi note-taking yang ditemukan

2022-10-26 04:50:03	2022-10-26 04:52:03	5	wsc01.id@gmail.com	Project Revenge	1. Siram tommy pakek air di toilet 2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari 3. Bocorin ban sepeda Laxus 4. tanya jasmine mo kerkol apa engga <3	1. Siram tommy pakek air di toilet 2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari 3. Bocorin ban sepeda Laxus 4. tanya jasmine mo kerkol apa engga <3	False	wsc01.id@gmail.com
------------------------	------------------------	---	--------------------	--------------------	--	--	-------	--------------------

Solution6(tommy)

Soal7

Challenge
0 Solves

7. Bobby Blunder

100

Bagian Ketujuh

Karena masih anak SMA, ternyata Bobby juga bisa saja teledor menyimpan sesuatu yang sifatnya rahasia dan gampang terekspos oleh publik karena pihak Anda berhasil mendapatkan sesuatu dari sana. Bobby telah menyimpan sebuah **backup password** yang ada pada aplikasi *note-taking* yang sama dengan sebelumnya. Apakah **isi konten** dari backup passwordnya?

Format: hUrUf@lay

Flag
Submit

Ternyata Bobby teledor menyimpan sebuah backup password yang berada di aplikasi note-taking kami disuruh menemukan apa isi konten dari backup password tersebut

2022-10-26 04:48:02	2022-10-26 04:49:30	4	wsc01.id@gmail.com	backup password	d4y3Lk_5N@GG123	d4y3Lk_5N@GG123	False	wsc01.id@gmail.com
------------------------	------------------------	---	--------------------	--------------------	-----------------	-----------------	-------	--------------------

Solution7(d4y3Lk_5N@GG123)

8. Detil Rencana

Scoreboard Challenges Notification

Challenge 0 Solves X

8. Detil Rencana

100

Bagian Kedelapan

Bobby merasa ketakutan karena kemampuan forensik Anda sangatlah handal. Anda ingin mengecek kapan **terakhir kali Bobby meng-update rencana jahatnya pada notes** yang telah dia buat **sebelumnya**. Apakah Anda dapat mengetahuinya?

Format jawaban (DD/MM/YYYY jam:menit WIB)

Contoh: 08/01/2007 12:37 WIB

Flag Submit

Kami disuruh mencari kapan terakhir kali bobby mengupdate rencana jahatnya pada notes dengan format yang disediakan kami menemukan waktu nya

2022-10-26 04:50:03	2022-10-26 04:52:03	5	wsc01.id@gmail.com	Project Revenge	1. Siram tommy pakek air di toilet 2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari 3. Bocorin ban sepeda Laxus 4. tanya jasmine mo kerkol apa engga <3	1. Siram tommy pakek air di toilet 2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari 3. Bocorin ban sepeda Laxus 4. tanya jasmine mo kerkol apa engga <3	False	wsc01.id@gmail.com
---------------------	---------------------	---	--------------------	-----------------	--	--	-------	--------------------

tapi setelah kami coba submit waktu seperti yang ada di aplikasi kami ternyata salah ,disitu kami bingung tapi firasat kami ini cuman beda waktu karena yang diminta adalah WIB sedangkan yang berada di ALEAPP kami tidak tahu zona waktu mana yang digunakan karena perbedaan zona waktu biasanya cuman di jam jadi kami mencoba mengubah jam-nya satu persatu dari 1-24 dan ternyata pada angka 11 itu adalah flagnya.

Solution8(26-10-2022 11:52 wib)

9. Sebelum Klimaks

Challenge

0 Solves

X

9. Sebelum Klimaks

100

Bagian Kesembilan

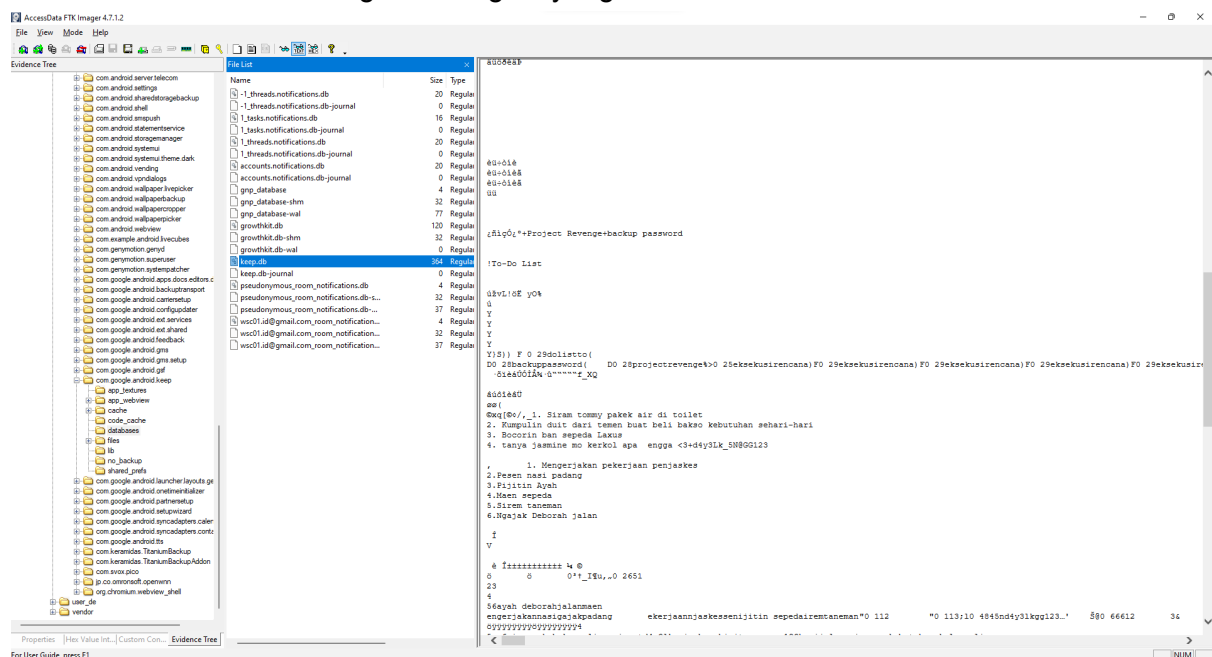
Bobby juga ternyata didapati bahwa ada **rencana jahat lainnya** yang ada pada **aplikasi note-taking yang sama** dengan sebelumnya NAMUN notes yang berisikan rencana jahat itu telah **DIHAPUS**. Anda sebagai tim Forensik tentunya tahu bahwa segala file yang dihapus pasti masih bisa dapat direcover dan dicek kembali apapun itu bukti digitalnya. Apa nama **judul** dari Notes yang telah ia hapus tersebut?

Format: judulnotestandanpaspasi

Flag

Submit

Kami sebagai team forensik harus bisa mendapatkan sebuah judul notes yang telah dihapus bobby,disini kami menggunakan tools FTK IMAGER dan menelusuri lagi di bagian Keep.db untuk mencari judul note yang dihapus ,setelah beberapa jam kami meneliti isi nya kami menemukan sebuah kecurigaan dibagian yang kami foto dibawah



kami menemukan sebuah string yaitu eksekusirencana yang kami duga itu adalah sebuah judul notes yang dihapus oleh bobby, setelah kami coba submit ternyata itu benar

Solution9(eksekusirencana)

Malicious

1. Shoulder Surfing 200

Semua Link file berlaku untuk semua challenge Memory Forensics. Silahkan akses dan download file di link ini:

https://drive.google.com/file/d/1ILdsJSYTKRiFXO6yOd_wlSzptuCu9es3/view?usp=sharing

Password:

saya_bUkan_8j0rka_tapi_g3n3rasi_emas_b4ngs4_Ind0nesia

Semua bagian soal kategori ini merupakan seri challenge "Malicious"

Bagian Pertama

Anda telah mendapati teman sekantor Anda tengah melakukan sesuatu yang cukup "malicious" pada victim host computer teman Anda dari CCTV. Sebelumnya, dia sedang melakukan shoulder surfing terhadap victim dan tim forensik mengira jika dia ingin mengingat kombinasi password temannya. Tatkala dikira itu sangatlah tidak mungkin, ternyata dia dapat mengakses komputernya dengan mudah. Beberapa menit kemudian, teman sekantor Anda tertangkap basah dan melarikan diri.

Dapatkan Anda mendapatkan **password logon OS** yang memang telah "diingat" oleh si penyerang? Tim Digital Forensik telah melakukan akuisisi memori pada laptop korban dan mereka meminta Anda untuk mengetes jika password tersebut bahkan **sangat mudah untuk didapatkan**.

Format: passwordnya

-

Diberikan VMEM oleh juri yang pertama kali kami lakukan adalah mengidentifikasi VMEM apa yang diberikan oleh juri menggunakan tools Volatility

```
PS D:\Latihan LKS> .\Volatility\volatilit.exe -f .\LKSN.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
      AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (D:\Latihan LKS\LKSN.vmem)
      PAE type : No PAE
      DTB : 0x187000L
      KDBG : 0xf80002bfc120L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0xffffffff80002bfe000L
      KUSER_SHARED_DATA : 0xffffffff7800000000L
      Image date and time : 2022-10-25 08:50:27 UTC+0000
      Image local date and time : 2022-10-25 15:50:27 +0700
PS D:\Latihan LKS>
```

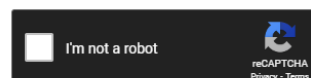
Yang diberikan adalah VMEM windows jadi disini kami langsung menjalankan command hivelist untuk melihat apa saja yang berada didalamnya dan tentu saja mata kami tertarik kepada MACHINE\SYSTEM dan CONFIG\SAM, jadi kami melakukan hexdump pada keduanya dan menyimpannya di komputer kami.

```
PS D:\Latihan LKS> .\Volatility\volatilit.exe -f .\LKSN.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
-----
0xffffffff8a001f07010 0x000000000f4cc010 \??\C:\Users\lksn\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffffffff8a004c32010 0x0000000025681010 \SystemRoot\System32\Config\DEFAULT
0xffffffff8a009fe1010 0x0000000021a2a010 \SystemRoot\System32\Config\SECURITY
0xffffffff8a00000f010 0x000000002d638010 [no name]
0xffffffff8a000024010 0x000000002d693010 \REGISTRY\MACHINE\SYSTEM
0xffffffff8a000054010 0x000000002d5b3010 \REGISTRY\MACHINE\HARDWARE
0xffffffff8a0013fb410 0x0000000022c00410 \SystemRoot\System32\Config\SOFTWARE
0xffffffff8a001424010 0x0000000014a40010 \Device\HarddiskVolume1\Boot\BCD
0xffffffff8a001677410 0x0000000021871410 \SystemRoot\System32\Config\SAM
0xffffffff8a00172f410 0x0000000018e43410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffffffff8a0017c0010 0x00000000187ac010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xffffffff8a001d39190 0x0000000008fc9190 \??\C:\System Volume Information\Syscache.hve
0xffffffff8a001f59010 0x000000007a102010 \??\C:\Users\lksn\ntuser.dat
PS D:\Latihan LKS> .\Volatility\volatilit.exe -f .\LKSN.vmem --profile=Win7SP1x64 hashdump -y 0xffffffff8a000024010 -s 0xffffffff8a001677410 > hashes.txt
Volatility Foundation Volatility Framework 2.6
```

Setelah mendapatkan hash yang tadi sudah kami temukan kami crack passwordnya dengan menggunakan web <https://crackstation.net/>

Enter up to 20 non-salted hashes, one per line:

6880c767cb7049dbd8d1234925cabb6d



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), Qubes/V3.1BackupDefaults

Hash	Type	Result
6880c767cb7049dbd8d1234925cabb6d	NTLM	happybirthday

Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

hashes.txt - Notepad

File Edit View

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:10eca58175d4228ece151e287086e824:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lksn:1001:aad3b435b51404eeaad3b435b51404ee:6880c767cb7049dbd8d1234925cabb6d:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:c78a69028265ae8f10aa485e8f19d0bb:::
```

Password (Flag) : happybirthday

2. Awal Mula

200

Bagian Kedua

Tim Digital Forensik melanjutkan investigasi dari apa yang dilakukan oleh penyerang di dalam komputer teman Anda, namun karena tim ini sedang sibuk mengurus event LKSN 2022, dapatkah Anda membantu mereka untuk menemukan proses apa yang menurut Anda sedang berjalan dan cukup malicious? Anda cukup mencantumkan *Process ID* -nya saja disini sebagai flagnya.

Di soal ke 2 diminta untuk menganalisis suatu proses yang malicious (mencurigakan) yang diminta adalah PID dari proses tersebut jadi kami menjalankan command ps list untuk melihat processlist apa saja yang berada didalam memori


```
PS D:\Latihan LKS> .\Volatility\volatilit.exe -f .\LKSN.vmem --profile=Win7SP1x64 pslist
```

Volatility Foundation Volatility Framework 2.6

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xffffffff8018dc2040	System	4	0	89	463	-----	0	2022-10-25 08:48:14 UTC+0000	
0xffffffff80197fd920	smss.exe	252	4	2	29	-----	0	2022-10-25 08:48:14 UTC+0000	
0xffffffff801a3ed060	csrss.exe	344	336	8	557	0	0	2022-10-25 08:48:18 UTC+0000	
0xffffffff801a6db060	wininit.exe	396	336	3	75	0	0	2022-10-25 08:48:18 UTC+0000	
0xffffffff801a6da4b0	csrss.exe	408	388	10	250	1	0	2022-10-25 08:48:18 UTC+0000	
0xffffffff801a6f7920	winlogon.exe	444	388	5	117	1	0	2022-10-25 08:48:19 UTC+0000	
0xffffffff801a70db00	services.exe	504	396	8	222	0	0	2022-10-25 08:48:19 UTC+0000	
0xffffffff801a75f700	lsass.exe	512	396	8	724	0	0	2022-10-25 08:48:19 UTC+0000	
0xffffffff801a75b320	lsn.exe	520	396	10	141	0	0	2022-10-25 08:48:19 UTC+0000	
0xffffffff801a7c9320	svchost.exe	608	504	11	359	0	0	2022-10-25 08:48:20 UTC+0000	
0xffffffff801a7e3b00	svchost.exe	672	504	7	297	0	0	2022-10-25 08:48:20 UTC+0000	
0xffffffff801a809690	svchost.exe	728	504	23	524	0	0	2022-10-25 08:48:20 UTC+0000	
0xffffffff801a83e5c0	svchost.exe	828	504	31	501	0	0	2022-10-25 08:48:21 UTC+0000	
0xffffffff801a862290	svchost.exe	880	504	32	786	0	0	2022-10-25 08:48:21 UTC+0000	
0xffffffff801a88d540	svchost.exe	916	504	41	866	0	0	2022-10-25 08:48:21 UTC+0000	
0xffffffff801a86bb00	audiobg.exe	984	728	7	133	0	0	2022-10-25 08:48:23 UTC+0000	
0xffffffff801a93db00	svchost.exe	516	504	22	401	0	0	2022-10-25 08:48:24 UTC+0000	
0xffffffff801a97bb00	spoolsv.exe	1120	504	17	284	0	0	2022-10-25 08:48:26 UTC+0000	
0xffffffff801a9deb00	svchost.exe	1148	504	20	320	0	0	2022-10-25 08:48:26 UTC+0000	
0xffffffff801a7ab310	svchost.exe	1244	504	11	147	0	0	2022-10-25 08:48:26 UTC+0000	
0xffffffff801aa8eb00	svchost.exe	1284	504	28	296	0	0	2022-10-25 08:48:26 UTC+0000	
0xffffffff801ab04b00	VGAAuthService.exe	1376	504	6	94	0	0	2022-10-25 08:48:27 UTC+0000	
0xffffffff801ab385f0	vmtoolsd.exe	1436	504	11	197	0	0	2022-10-25 08:48:27 UTC+0000	
0xffffffff801ab93b00	svchost.exe	1700	504	7	95	0	0	2022-10-25 08:48:29 UTC+0000	
0xffffffff801abc7b00	dllhost.exe	1864	504	20	196	0	0	2022-10-25 08:48:29 UTC+0000	
0xffffffff801ac6fb00	WmiPrvSE.exe	1916	608	10	188	0	0	2022-10-25 08:48:29 UTC+0000	
0xffffffff801aaba060	dllhost.exe	1968	504	18	201	0	0	2022-10-25 08:48:30 UTC+0000	
0xffffffff801acd18f0	msdtc.exe	120	504	15	156	0	0	2022-10-25 08:48:31 UTC+0000	
0xffffffff801ad1fb00	VSSVC.exe	1224	504	7	120	0	0	2022-10-25 08:48:35 UTC+0000	
0xffffffff801a348060	WmiPrvSE.exe	2116	608	14	318	0	0	2022-10-25 08:48:49 UTC+0000	
0xffffffff801ae7fb00	taskhost.exe	2336	504	11	204	1	0	2022-10-25 08:48:55 UTC+0000	
0xffffffff801aea9940	dwm.exe	2404	828	6	76	1	0	2022-10-25 08:48:56 UTC+0000	
0xffffffff801ae44060	explorer.exe	2480	2396	41	998	1	0	2022-10-25 08:48:56 UTC+0000	
0xffffffff801a6c060	vm3dservice.exe	2624	2480	6	42	1	0	2022-10-25 08:48:58 UTC+0000	
0xffffffff801afa4060	vmtoolsd.exe	2640	2480	8	186	1	0	2022-10-25 08:48:58 UTC+0000	
0xffffffff801b00ab00	appsiory.exe	2660	2480	9	121	1	1	2022-10-25 08:48:59 UTC+0000	
0xffffffff801a822b00	WmiApSrv.exe	2796	504	6	119	0	0	2022-10-25 08:49:03 UTC+0000	
0xffffffff801b033b00	SearchIndexer.exe	2948	504	14	552	0	0	2022-10-25 08:49:06 UTC+0000	
0xffffffff801a6e8b00	svchost.exe	2472	504	12	359	0	0	2022-10-25 08:49:08 UTC+0000	
0xffffffff801a817230	wmpnetwk.exe	2592	504	17	438	0	0	2022-10-25 08:49:09 UTC+0000	
0xffffffff8019873060	notepad.exe	1532	2480	2	62	1	0	2022-10-25 08:49:50 UTC+0000	
0xffffffff801a984b00	notepad.exe	2844	2480	2	62	1	0	2022-10-25 08:49:57 UTC+0000	
0xffffffff80198401d0	cmd.exe	1128	2480	1	23	1	0	2022-10-25 08:50:17 UTC+0000	
0xffffffff8019836430	conhost.exe	1740	408	3	54	1	0	2022-10-25 08:50:17 UTC+0000	
0xffffffff8019cc2440	softwareupdate	3004	1128	1	13	1	0	2022-10-25 08:50:21 UTC+0000	
0xffffffff801ac5cb00	dllhost.exe	1536	608	7	94	1	0	2022-10-25 08:50:22 UTC+0000	
0xffffffff801ac78b00	cmd.exe	1788	1436	0	-----	0	0	2022-10-25 08:50:27 UTC+0000	2022-10-25 08:50:27 UTC+0000
0xffffffff801ac78060	conhost.exe	2980	344	0	30	0	0	2022-10-25 08:50:27 UTC+0000	2022-10-25 08:50:27 UTC+0000

Mata kami tertuju kepada softwareupdate karena nama process file dari ini sangatlah jauh berbeda dengan yang lain dan juga biasanya windows tidak melabelkan update mereka dengan 'softwareupdate'. Untuk memastikan analisa kami kami melakukan dlllist pada process tersebut untuk melihat apa saja yang dieksekusi dari program tersebut

```
PS D:\Latihan LKS> .\Volatility\volatilit.exe -f .\LKSN.vmem --profile=Win7SP1x64 dlllist -p 3004
```

Volatility Foundation Volatility Framework 2.6

softwareupdate pid: 3004

Command line : .\softwareupdateyeyy.exe

Service Pack 1

Base	Size	LoadCount	Path
0x0000000000400000	0xad000	0xffff	C:\Users\lksn\Desktop\softwareupdateyeyy.exe
0x00000000772d0000	0x19f000	0xffff	C:\Windows\SYSTEM32\ntdll.dll
0x00000000770b0000	0x11f000	0xffff	C:\Windows\system32\kernel32.dll
0x000007feffd10000	0x6a000	0xffff	C:\Windows\system32\KERNELBASE.dll
0x000007feff150000	0x9f000	0xffff	C:\Windows\system32\msvcrt.dll

PS D:\Latihan LKS>

Benar saja ada softwareupdateyeyy.exe yang pastinya bukan lah dari system melainkan malware yang ditanam.

PID (Flag) : 3004