Analisis Aktivitas User Melalui Windows Registry

Ewaldo S.H., Nur Amin K., Teguh H., Farid D. H.

Abstrak

Ketergantungan yang tinggi dengan teknologi informasi menyebabkan banyak aspek kehidupan tidak lagi dapat dilihat terpisah dari teknologi informasi. Hal ini juga berarti semakin tingginya kejahatan yang terkait ataupun menggunakan teknologi informasi sebagai sarana kejahatan. Kemampuan memahami aktivitas seseorang dalam tataran teknologi informasi akan semakin memegang peranan penting dalam memecahkan berbagai jenis kejahatan terkait teknologi informasi. Tulisan ini akan membahas bagian dari windows registry yang dianggap memegang peranan besar bagi seorang analis forensik digital untuk memahami user activity.

Index Term: registry, digital forensic, information security

I. PENGANTAR

Tingginya penggunaan teknologi informasi, melahirkan sebuah era baru, yaitu "*information economy*". Beberapa penggerak utama dari *information economy* tersebut adalah[1]:

1. globalisasi pasar, produk dan sumber daya;
2. Intensitas informasi elektronik; dan
3. Peningkatan secara geometrik level dari keterhubungan elektronik.

information economy mengakibatkan ketergantungan yang tinggi antara dunia industri dengan teknologi informasi. Ketergantungan atas teknologi informasi ini tentu saja tidak lepas dari penggunaan *hardware*, *software*. *Operating system* sebagai bagian dari *software* menjadi sarana sebuah *hardware* dapat digunakan oleh *user* sehingga dapat bernilai ekonomi.

Operating system sendiri memiliki beberapa bagian didalamnya. Memahami bagian dari *operating system* sendiri, merupakan kunci dari memahami aktivitas *user*. Salah satu bagian dari *operating system*, khususnya pada *operating system windows,* adalah *registry.*

Registry digunakan untuk mengatur berbagai konfigurasi pada *operating system.* Alat yang digunakan untuk mengatur konfigurasi tersebut mulai dari versi awal Windows (3.1, 3.11, dst)

[1] Calder, Alan. "IT governance: A manager's guide to data security and ISO 27001/ISO 27002." (2008).

berbentuk terpisah-pisah dan tersebar pada beberapa file konfigurasi berbentuk *autoexec.bat, config.sys, win.ini* dan *system.ini*[2], namun secara umum terdapat trend sentralisasi untuk keseluruhan *file-file* yang digunakan untuk pengaturan konfigurasi pada operating sistem Windows.

Pada kondisinya sekarang, sebuah Windows registry sendiri adalah sebuah database hirarkis yang terpusat dan berfungsi menyimpan informasi terkait pengguna (*users*), perangkat keras dan aplikasi yang terpasang.

Registry dan Aktivitas User

Sebagai bagian dari *operating system* yang salah satu kegunaannya untuk menyimpan informasi terkait pengguna, maka *registry* memiliki nilai bukti yang cukup tinggi, khususnya pada sebuah pemeriksaan forensik digital yang memiliki fokus pada aktivitas *user*. Sehingga sebuah pemeriksaan forensik digital yang lengkap terhadap sebuah *operating system* haruslah melibatkan pemeriksaan atas *registry file* dari *operating system* tersebut.

Seperti yang disampaikan penulis bahwa registry sendiri tidak hanya mencatat hal dan konfigurasi terkait user, namun juga terkait konfigurasi perangkat keras dan perangkat lunak, tulisan ini akan berfokus pada beberapa konfigurasi (baik *user*, perangkat keras, atau perangkat lunak) yang erat kaitanya dengan kegiatan/ aktivitas *user* pada device tersebut.

Struktur Registry

Windows registry dapat diakses dengan menggunakan perangkat lunak bawaan windows bernama regedit.

Registry adalah sebuah database hierarkis, dan terstruktur dalam sebuah bentuk pohon. Setiap simpul dalam pohon tersebut disebut *key,* sedangkan setiap *key* dapat berisi *key* lain (*subkey*) atau *values*. Bagian pertama yang terlihat ketika menjalankan regedit adalah adanya lima buah “folder” teratas yang disebut dengan registry hive (atau disebut juga root key).

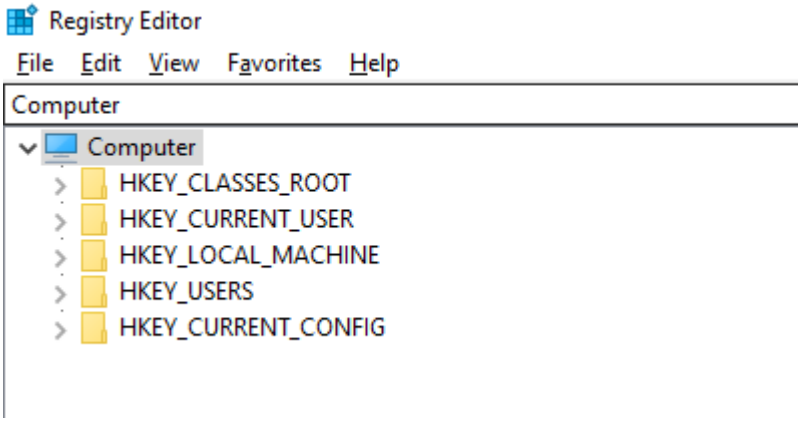
II. TULISAN TERKAIT

Tulisan mengenai windows registry sudah cukup banyak, dan membahas dari berbagai segi yang beragam. Salah satu tulisan paling awal yang membahas secara lengkap registry adalah Harlan Carvey yang menggambarkan windows registry sebagai salah satu bukti yang dapat

[2] terdapat pula berbagai file konfigurasi yang dimiliki perangkat lunak

dipertimbangkan dalam sebuah pemeriksaan forensik digital.Khawla et. al. membahas secara khusus windows registry pada Windows 7, Zhu et. al. memfokuskan penelitian pada aspek temporal dari MRU key. Selain peneliti diatas, terdapat pula Farmer yang merinci beberapa key registry yang dianggap penting dalam sebuah pemeriksaan forensik,[3] serta menggabungkan hasil penelitian lain dalam sebuah tulisan yang membahas registry key secara umum sebagai panduan bagi pemeriksa forensik[4].

Selain dalam bentuk *paper* terdapat beberapa tulisan berformat buku yang kerap menjadi rujukan dalam kegiatan pemeriksaan forensik digital terkait dengan windows registry. Carvey, paling tidak, memiliki dua buah buku yang menjadi rujukan. Keduanya membahas secara mendalam windows forensic[5] dan tools analisis windows forensic[6], dengan menyertakan pembahasan konsep registry yang cukup teknis dan dapat digunakan untuk pemeriksaan forensik digital.



Masing-masing hive tersebut memiliki peran masing-masing dalam mendukung jalannya sistem operasi. HKEY_USERS (HKU) menyimpan informasi terkait *user profile* yang ter-*load* dalam sebuah sistem operasi yang berjalan. HKEY_CURRENT_USER (HKCU) adalah menyimpan bagian informasi dari HKU, yaitu informasi terkait *user* yang sedang *logged in* dalam sistem operasi yang berjalan. HKEY_LOCAL_MACHINE (HKLM) menyimpan informasi terkait perangkat (keras dan lunak) yang terdapat dalam sebuah sistem. HKEY_CURRENT_CONFIG (HKCC) menyimpan informasi konfig sistem, sedangkan HKEY_CLASSES_ROOT (HKCR) menyimpan informasi tentang *program default* untuk membuka sebuah file.

---

[3] Farmer, Derrick J., and V. Burlington. "A forensic analysis of the Windows registry." *Champlain College Burlington, Vermont* (2007).

[4] Farmer, Derrick J., and V. Burlington. "A Windows registry quick reference: for the everyday examiner." *Forensic Focus* (2007): 1-14.

[5] Carvey, Harlan. *Windows registry forensics: Advanced digital forensic analysis of the windows registry*. Elsevier, 2011.

[6] Carvey, Harlan. *Windows forensic analysis DVD toolkit*. Syngress, 2018.

HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, dan HKEY_CLASSES_ROOT merupakan hive alias dari beberapa key registry dari HKEY_USERS dan HKEY_LOCAL_MACHINE. Artinya hive-hive tersebut hanya merupakan referensi kepada beberapa key yang berada di hive HKEY_USERS dan HKEY_LOCAL_MACHINE.

III. METODOLOGI

Tulisan ini akan mendokumentasikan bagaimana sebuah kegiatan yang dilakukan *user* meninggalkan jejak, khususnya pada *registry*. Hasil dokumentasi tersebut diharapkan dapat digunakan oleh analis forensik digital untuk mendapatkan gambaran kegiatan atau aktivitas yang dilakukan *user*.

Untuk mencapai tujuan ini, terdapat beberapa teknik analisis forensik digital yang dapat digunakan. Tulisan ini akan menggunakan konsep teknik analisis malware dinamis dasar (*basic malware analysis*) dengan menggunakan beberapa penyesuaian, mengingat kegiatan yang dilakukan pengujian bukan merupakan *malware* namun merupakan program biasa.

Sikorski dan Honig pada buku practical malware analysis, untuk melakukan *basic dynamic malware analysis* menggunakan beberapa perangkat berikut:

a. Virtual Machine (virtualbox) sebagai environment,
b. Process Monitor (procmon) dan Process Explorer (procexp) untuk memantau proses,
c. Dependency Walker untuk memantau penggunaan *dynamic link library* (.dll),
d. Regshot untuk memantau akses dan perubahan terhadap registry,
e. ApateDNS, Netcat, Inetsim untuk simulasi network.

Dikarenakan sifat tulisan yang sedikit berbeda dengan analisis *malware* biasa, tulisan ini akan memfokuskan diri pada windows registry dan proses. Pemantauan proses dilakukan dengan procmon dan procexp (sesuai kebutuhan) serta Registry Change View[7] digunakan untuk memantau akses dan perubahan terhadap registry, hal ini dikarenakan *regshot* sudah cukup lama tidak memperoleh pembaruan sehingga terasa kurang mudah digunakan.

Serupa dengan *basic malware analysis*, rangkaian kegiatan yang dilakukan untuk memantau perubahan yang disebabkan aktivitas user adalah sebagai berikut:

a. Mendokumentasikan kondisi awal registry,
b. Melakukan kegiatan/ aktivitas *user* yang akan dipantau,
c. Mendokumentasikan kondisi akhir registry,

[7] "Compare Snapshots of Windows Registry." NirSoft, Nirsoft, www.nirsoft.net/utils/registry_changes_view.html. Accessed 22 Nov. 2021.

d. Mendokumentasikan hasil pemantauan proses (apabila diperlukan).
e. Membandingkan kondisi awal dan akhir registry.

IV. PEMBAHASAN

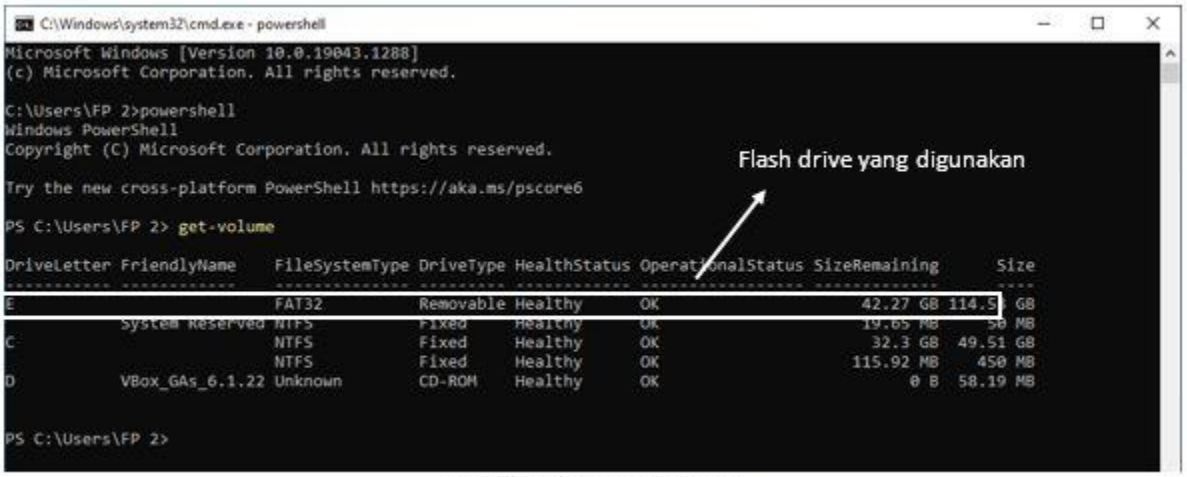
Terdapat beberapa aktivitas user yang akan dilakukan, serta terhadap perubahan atas registry yang disebabkan aktvitas tersebut, akan di dokumentasikan sampai dengan level *registry key*, dan *value key* yang terpengaruh. Tulisan ini akan berfokus pada dua aktivitas yang sangat terkait dengan e-discovery, yaitu melakukan koneksi USB devices dan menjalankan sebuah portable executable (PE files).

Melakukan koneksi *USB Devices*

Percobaan ini dilakukan menggunakan bantuan aplikasi RegistryChangesView v1.28 dengan cara merekam kondisi awal *registry* kemudian memasang media baru berupa *flash drive* setelah itu merekam kembali kondisi *registry*. Aplikasi RegistryChangesView selanjutnya menampilkan *registry* mana saja yang berubah yang diakibatkan pemasangan *flash drive* tersebut.

Media *flash drive* yang digunakan sebagaimana pada informasi dibawah ini.

Gambar 1-Informasi media flash drive



Gambar 2-Informasi dirve letter

Informasi yang didapatkan atas *flash drive* yang dipasang adalah:

Model : SanDisk Ultra USB Device

Serial Number : 4C530001271030109510

Volume Name (Drive Letter) : E

Dari percobaan yang dilakukan atas media *flash drive* diatas terdapat 504 *registry key* yang berubah menurut aplikasi RegistryChangesView. Adapun setelah dilakukan penyederhanaan, *registry* yang berubah adalah sebagaimana pada tabel berikut.

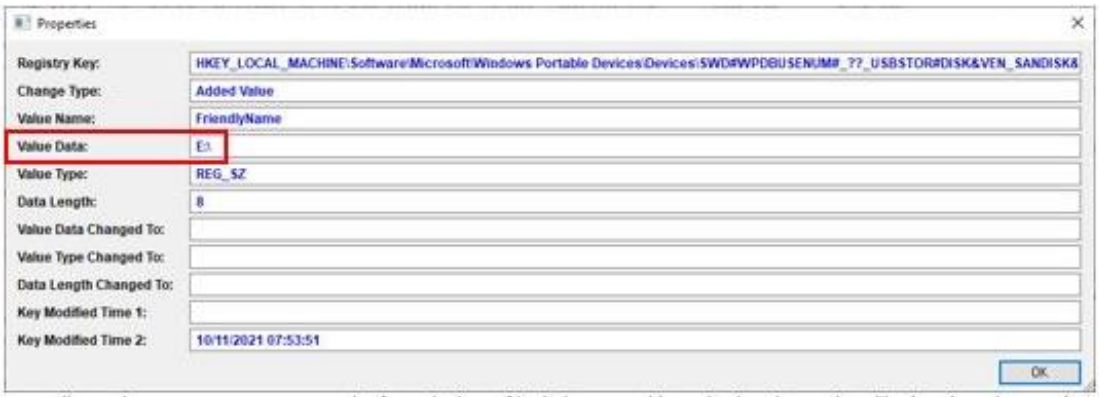
No	Registry Key
1	HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData
2	HKEY_CURRENT_USER\SOFTWARE\Microsoft\OneDrive\Accounts
3	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ActivityDataModel\ReaderRevisionInfo
4	HKEY_LOCAL_MACHINE\Software\Microsoft\Multimedia\Audio\Journal
5	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Notifications\Data
6	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Portable Devices\Devices
7	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles
8	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\StorageSense\Parameters
9	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\VFUProvider
10	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Orchestrator\Scheduler
11	HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Class
12	HKEY_LOCAL_MACHINE\System\ControlSet001\Control\DeviceClasses
13	HKEY_LOCAL_MACHINE\System\ControlSet001\Control\DeviceContainers
14	HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\Volume
15	HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\SWD\WPDBUSENUM
16	HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB
17	HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR
18	HKEY_LOCAL_MACHINE\System\ControlSet001\Services\bam\State\UserSettings
19	HKEY_LOCAL_MACHINE\System\MountedDevices

Tabel 1-Tabel Registry Key yang sudah dilakukan penyederhanaan tampilan

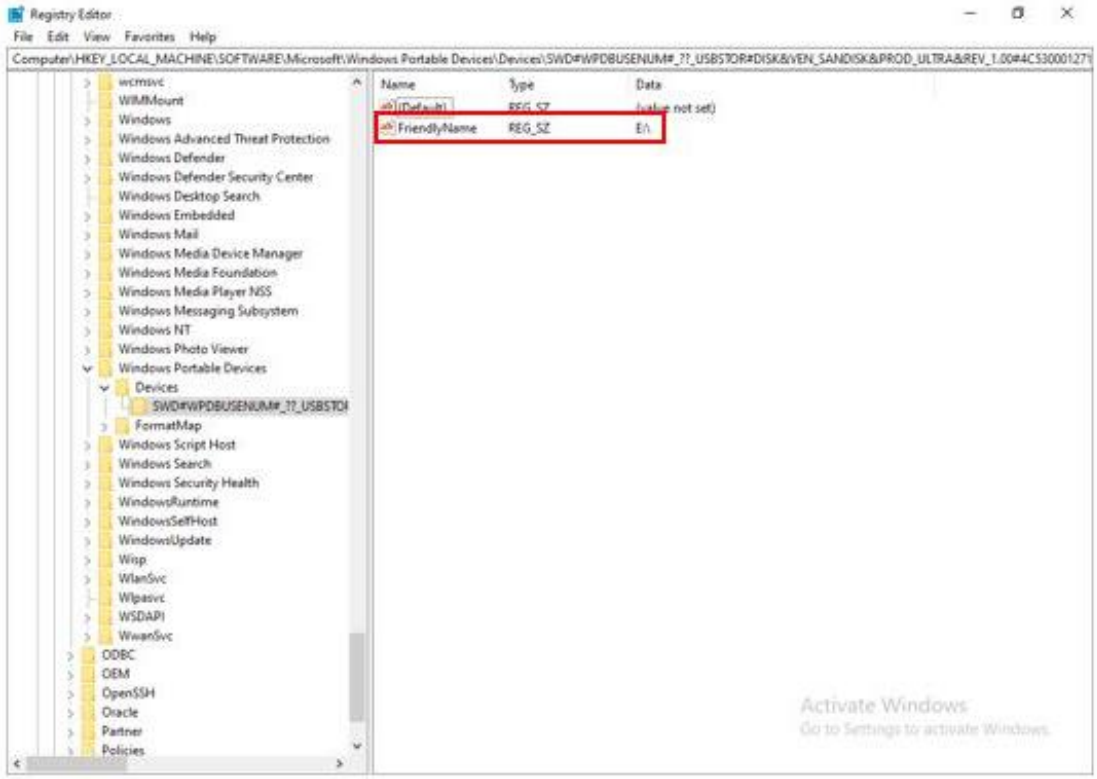
Selanjutnya dilakukan penelusuran untuk mengetahui *registry* yang berubah dikarenakan aktifitas pemasanagan *flash drive. Registry* yang memuat informasi atas *flash drive* adalah sebagai berikut.

1. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Portable Devices\Devices

   Pada *registry key* ini terdapat informasi data yang menunjukkan *volume name* E:\ dimana *volume* tersebut merupakan *volume name* dari *flash drive* yang dipasang.



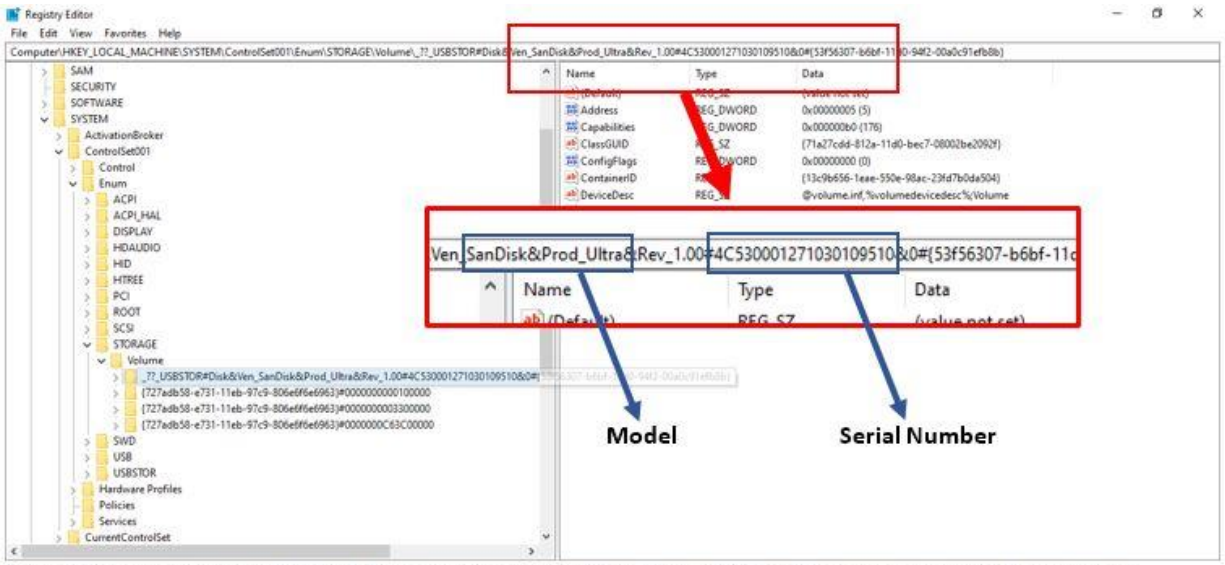
Gambar 3-Tampilan registry HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Portable Devices\Devices pada aplikasi RegistryChangesView



Gambar 4-Tampilan registry HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Portable Devices\Devices pada aplikasi Registry Editor

2. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\Volume

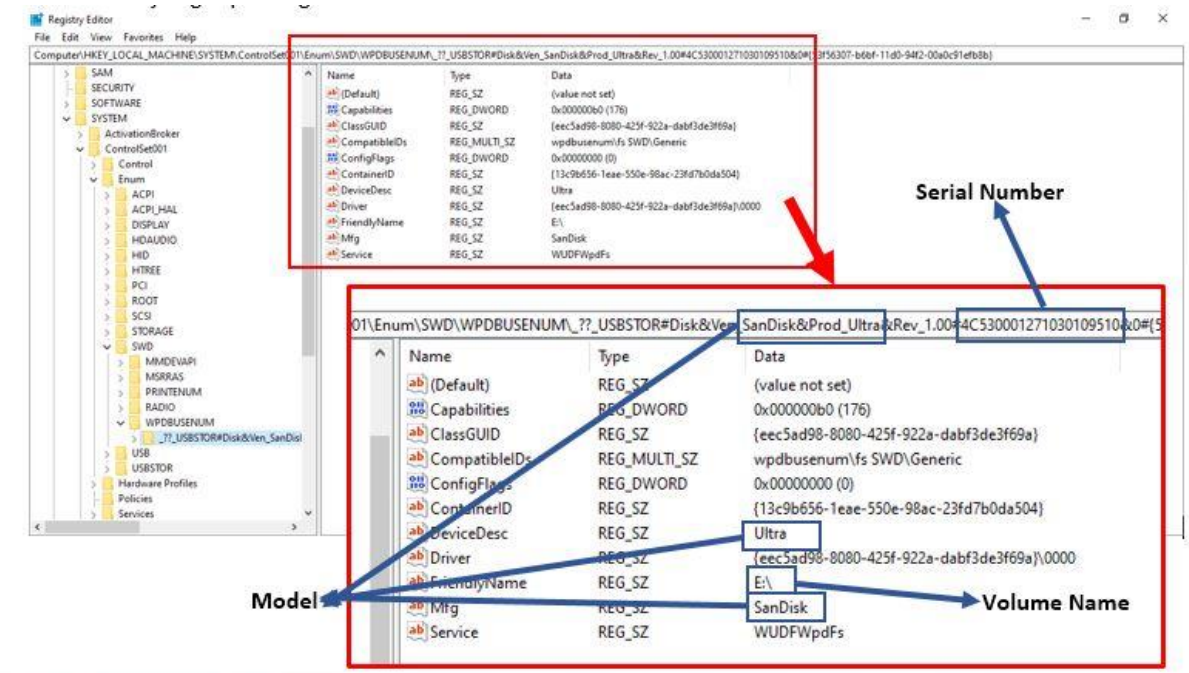
Pada *registry key* ini terdapat informasi data yang menunjukkan model dan *serial number* dari *flash drive* yang dipasang.



Gambar 5-Tampilan registry HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\Volume pada aplikasi Registry Editor

3. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\SWD\WPDBUSENUM

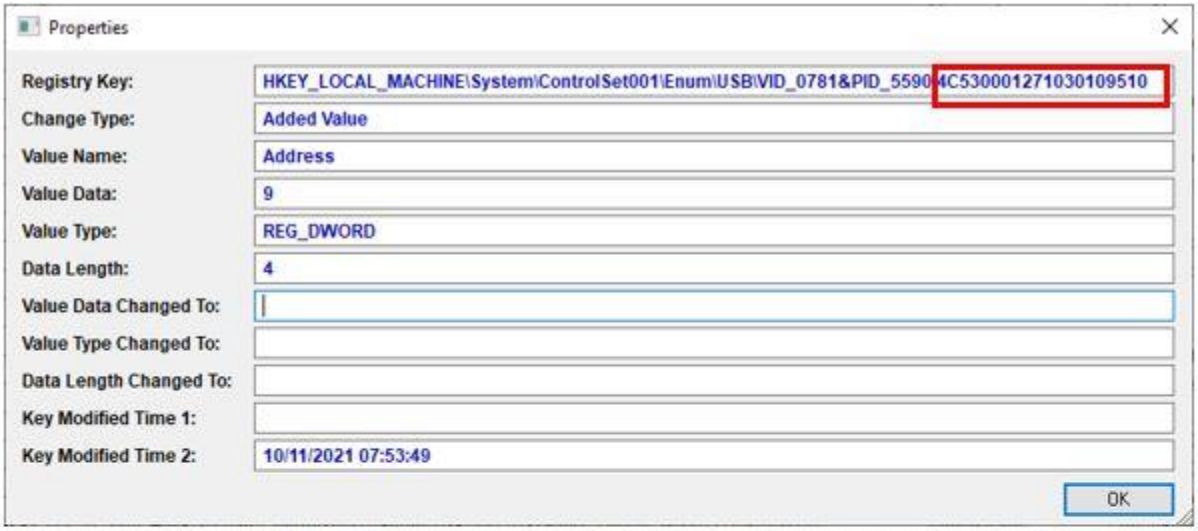
Pada *registry key* ini terdapat informasi data yang menunjukkan model, *serial number* dan *volume name* dari *flash drive* yang dipasang.



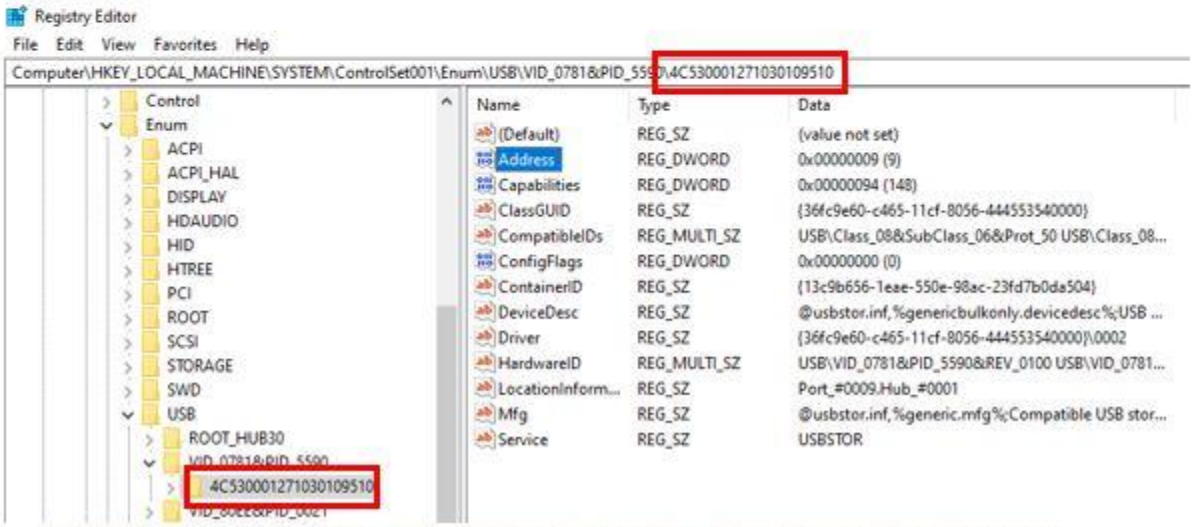
Gambar 6-Tampilan registry HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\SWD\WPDBUSENUM pada aplikasi Registry Editor

4. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB

Pada *registry key* ini terdapat informasi data yang menunjukkan *serial number* dari *flash drive* yang dipasang.



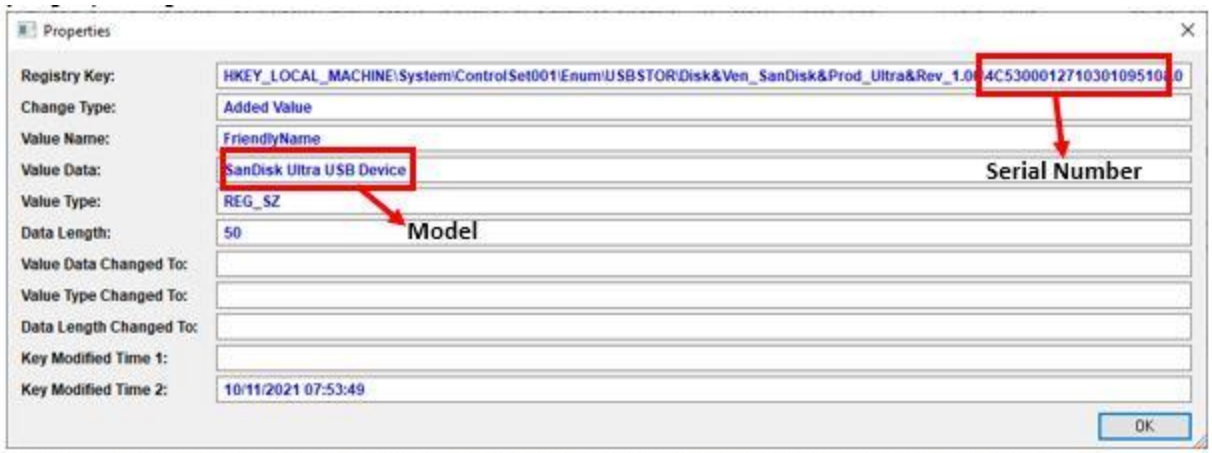
Gambar 7-Tampilan registry HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB pada aplikasi RegistryChangesView



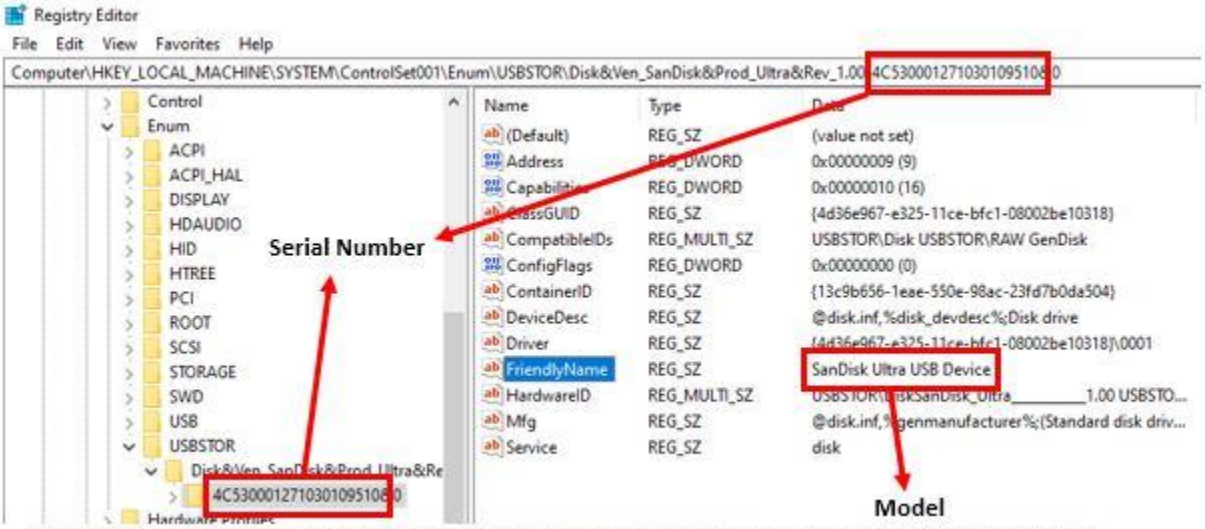
Gambar 8-Tampilan registry HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB pada aplikasi Registry Editor

5. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR

Pada *registry key* ini terdapat informasi data yang menunjukkan model dan *serial number* dari *flash drive* yang dipasang.



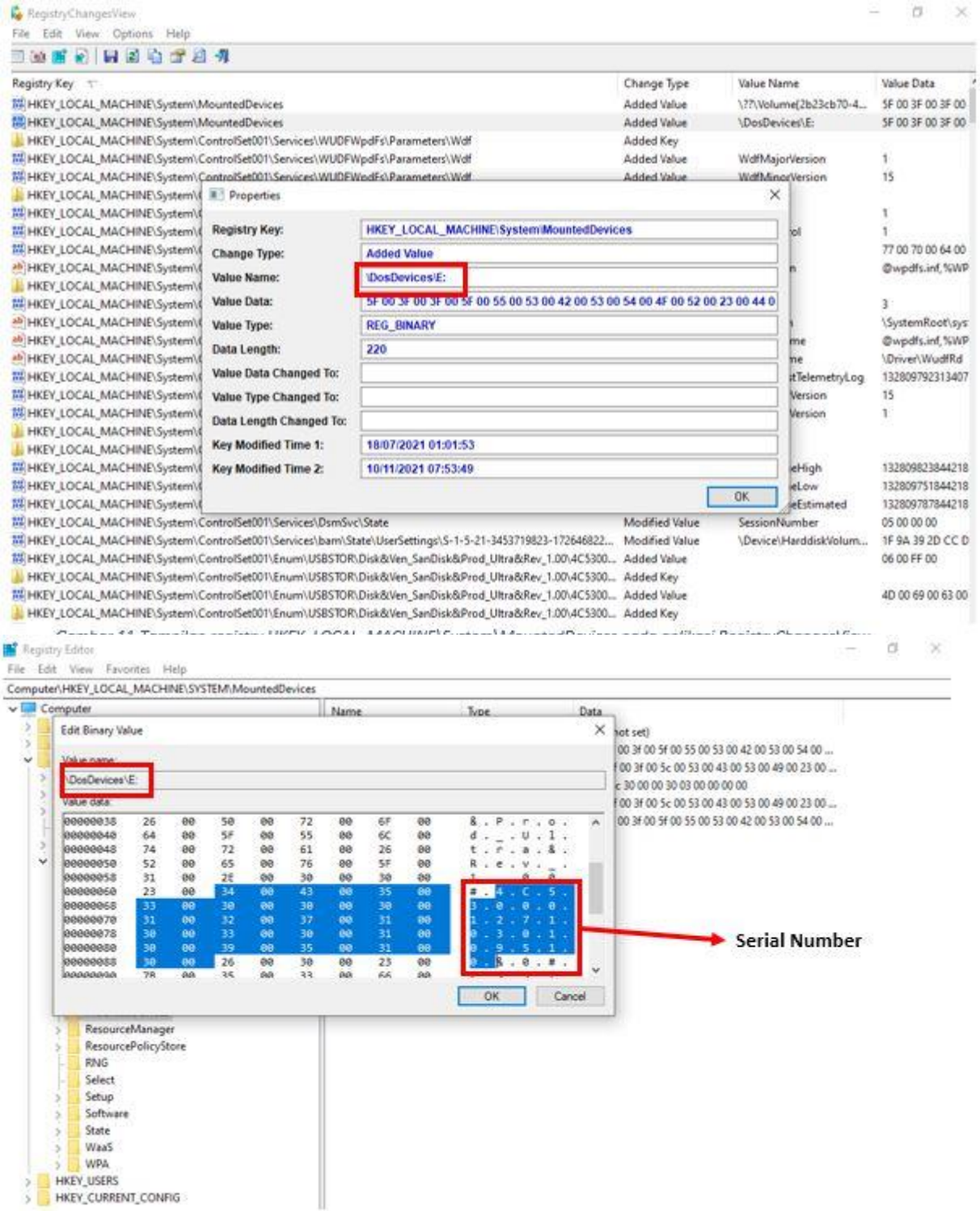
Gambar 9-Tampilan registry HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR pada aplikasi RegistryChangesView



Gambar 10-Tampilan registry HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR pada aplikasi Registry Editor

6. HKEY_LOCAL_MACHINE\System\MountedDevices

Pada *registry key* ini terdapat informasi data yang menunjukkan *serial number* dari *flash drive* yang dipasang dan mengarah ke volume E.



Gambar 12-Tampilan registry HKEY_LOCAL_MACHINE\System\MountedDevices pada aplikasi Registry Editor

Berdasarkan percobaan yang dilakukan diatas didapatkan 6 *registry keys* yang berubah saat dilakukan pemasangan *USB device* berupa *flash drive,* yaitu:

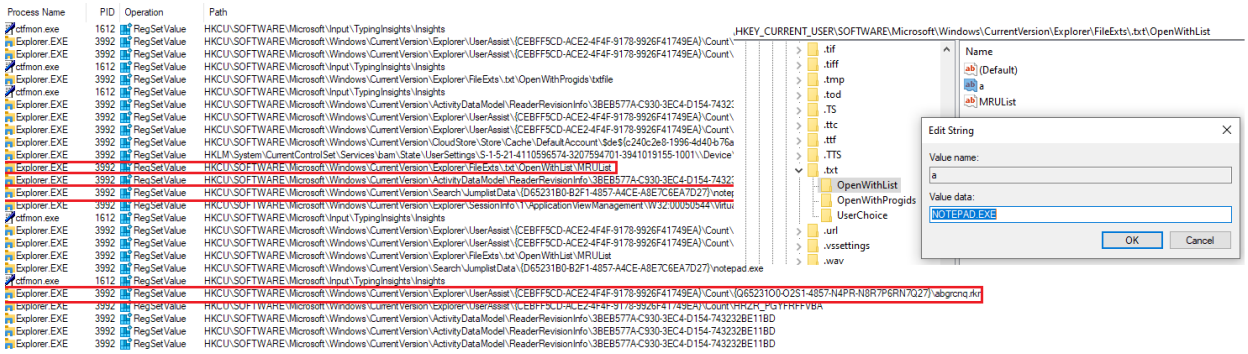
1. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Portable Devices\Devices
2. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\STORAGE\Volume
3. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\SWD\WPDBUSENUM
4. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USB
5. HKEY_LOCAL_MACHINE\System\ControlSet001\Enum\USBSTOR
6. HKEY_LOCAL_MACHINE\System\MountedDevices

Menjalankan Portable Executable (PE)

Pada kegiatan ini PE notepad.exe akan dijalankan melalui beberapa cara yang berbeda, serta dilakukan pencatatan pada perubahan registry dari beberapa cara berbeda tersebut. Untuk mencatat perubahan pada registry, digunakan process monitor[8] dan dilakukan filter hanya terhadap operasi "RegSetValue" atau operasi dimana terjadi perubahan pada registry, serta cyberchef[9] untuk melakukan konversi pada data yang ditemukan.

Menjalankan portable executable (PE) dengan *double click* file *default*

Pada kegiatan ini PE notepad.exe akan dijalankan melalui *double click* pada sebuah file txt (*text file*) yang secara default akan menggunakan notepad.exe untuk membukanya.

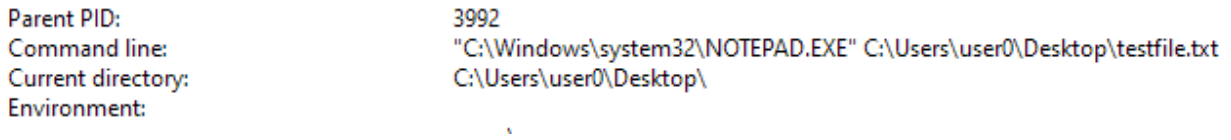


gambar 13 – registry key terpengaruh

explorer.exe terlihat melakukan perubahan pada beberapa registry key, sebelum menjalankan notepad. Notepad sendiri dijalankan dengan parent process id 3992, yaitu parent process id milik explorer.exe.

[8] Markruss. "Process Monitor - Windows Sysinternals." Microsoft Docs, 16 Dec. 2021, docs.microsoft.com/en-us/sysinternals/downloads/procmon.

[9] "CyberChef." *Crown Copyright 2016*, gchq.github.io/CyberChef. Accessed 24 Dec. 2021.



gambar 14 - parent process ID notepad

Terdapat beberapa registry key yang terpengaruh langsung dengan aktivitas yang dilakukan. yaitu:

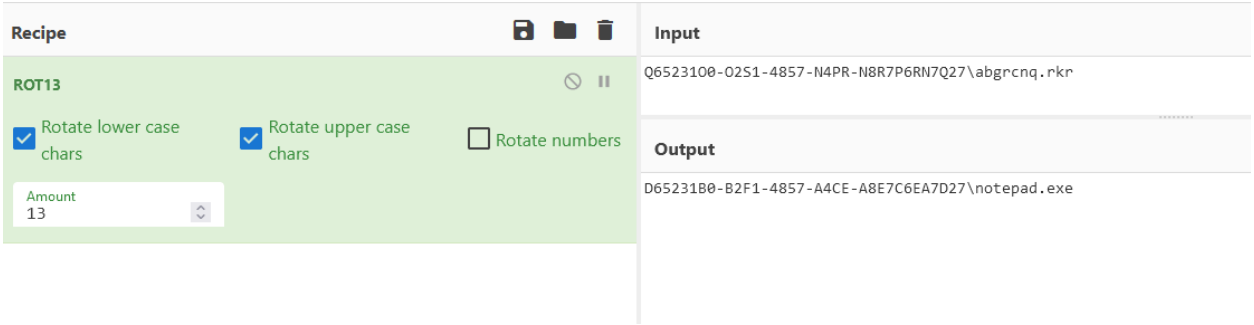
1. HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-4110596574-3207594701-3941019155-1001\\Device\HarddiskVolume2\Windows\System32\notepad.exe
2. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt\OpenWithList\MRUList
3. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\notepad.exe
4. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q65231O0-O2S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr

Registry key 1, merupakan registry key yang berubah apabila background activity monitor (BAM) mencatat adanya PE yang dijalankan. BAM baru tersedia sejak Windows 10 v1709 dan tidak ditemukan pada versi sebelumnya.

Registry key 2 dan 3 merupakan registry yang terkait dengan ekstensi file (karena menjalankan file langsung, dan bukan menjalankan PE)

Registry key 4 tercatat *encoded* dengan menggunakan rot13[10] dan digunakan cyberchef untuk men-*decode* data tersebut sebagaimana terlihat pada gambar 15. Sehingga diperoleh value “D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27\notepad.exe”. Bagian pertama dari value tersebut merupakan known folder id yang merujuk ke “%windir%\system32“[11]. Sedangkan key “CEBFF5CD-ACE2-4F4F-9178-9926F41749EA” pada registry key ke 4 merupakan registry key yang merupakan referensi kepada file atau sebuah objek.

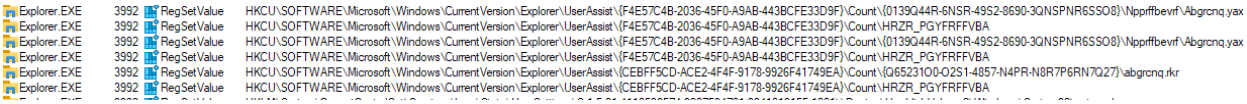
[10] “ROT13 Is Used in Windows? You’re Joking!” *Didier Stevens*, 24 July 2006, blog.didierstevens.com/2006/07/24/rot13-is-used-in-windows-you%E2%80%99re-joking.
[11] Jwmsft. “KNOWNFOLDERID (Knownfolders.h) - Win32 Apps.” *Microsoft Docs*, 21 Aug. 2021, docs.microsoft.com/en-us/windows/win32/shell/knownfolderid.



gambar 15 – cyberchef dengan rot13

Menjalankan portable executable (PE) dengan menjalankan *shortcut*

Berbeda dengan kegiatan sebelumnya, pada kegiatan ini PE notepad.exe akan dijalankan dengan menggunakan shortcut (pada *start menu*) dan tanpa membuka file apapun.



gambar 16 – menjalankan PE via shortcut

Hasil dari kegiatan ini mengubah registry key berikut:

1. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Npprffbevrf\Abgrcnq.yax
2. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q65231O0-O2S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr

Terdapat sedikit perbedaan registry key yang terpengaruh dengan kegiatan sebelumnya. Pada bagian ini registry key yang terkait dengan ekstensi file (sebelumnya registry key 2 dan 3) tidak muncul. Serta muncul sebuah registry key baru yaitu “F4E57C4B-2036-45F0-A9AB-443BCFE33D9F”.

Registry key 2 dengan menggunakan metode yang sama seperti sebelumnya, dapat di decode menjadi “%windir%\system32\notepad.exe”.

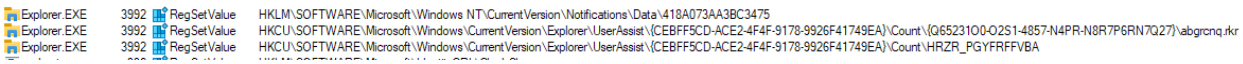
Sedangkan registry key 1 dapat di decode menjadi “0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8\ Accessories\Notepad.lnk”. Bagian pertama dari hasil decoding tersebut, seperti sebelumnya, merupakan known shell folder id [12] yang merujuk kepada “%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs”. Sedangkan bagian kedua

[12] Jwmsft. “KNOWNFOLDERID (Knownfolders.h) - Win32 Apps.” *Microsoft Docs*, 21 Aug. 2021, docs.microsoft.com/en-us/windows/win32/shell/knownfolderid.

membutuhkan decoding rot13, sehingga secara penuh *path*-nya merujuk kepada "%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Notepad.lnk". terlihat juga bahwa jenis file yang tertampil berekstensi lnk dan bukan exe.

Menjalankan portable executable (PE) langsung

Pada bagian ketiga PE akan dijalankan langsung, dengan melakukan *double click* pada icon notepad.exe.



gambar 17 – menjalankan PE langsung

pada bagian terakhir ini, dilakukan filter untuk menemukan semua registry yang berubah semenjak dijalankan PE notepad.exe. Tidak ditemukan registry key "F4E57C4B-2036-45F0-A9AB-443BCFE33D9F" yang sebelumnya kita catat merupakan referensi untuk shortcut.

Melainkan tercantum registry key yang merupakan referensi kepada sebuah file/ objek berikut:

1. "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q65231O0-O2S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr"

dengan menggunakan pola decode rot13 seperti sebelumnya, maka kita mendapatkan "{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\notepad.exe", dimana bagian pertamanya merupakan known shell folder id yang merujuk ke "%windir%\system32\notepad.exe".

Konsiderasi tentang waktu

Pada setiap perubahan pada *registry key* (bukan *registry value*) yang dibahas sebelumnya, dilakukan pencatatan atas *last write time*, yang dapat di lihat dengan melakukan ekspor (dengan jenis txt) via regedit, atau menggunakan perangkat analisis registry. Hal ini dapat menjadi sarana untuk melakukan analisis temporal atas aktivitas user.

V. PENUTUP

Melalui tulisan ini terlihat bahwa, kegiatan user melakukan koneksi USB *devices* mempengaruhi setidaknya enam buah *registry keys*, sedangkan menjalankan *portable executables* mempengaruhi satu sampai dengan empat *registry keys,* tergantung dari bagaimana *user* melakukan eksekusi file tersebut.

Tulisan ini menyentuh beberapa aspek dari aktivitas *user* pada *registry*, sehingga masih terdapat beberapa topik yang dapat ditelaah lebih dalam, serta menjadi pelengkap bagi tulisan ini, antara lain masih banyak terdapat *key* dan *subkey* lain dari *registry* yang dapat dibahas. Selain itu terdapat beberapa bagian lain diluar *registry* yang dapat melengkapi pengetahuan kita terkait aktivitas *user*. Terakhir adanya sebuah *script incident response* yang dapat melakukan akuisisi atas keseluruhan *registry* dan bagian di luar *registry* yang terkait langsung dengan aktivitas *user,* dapat menjadi sarana standarisasi penanganan alat bukti elektronik.

REFERENCES

1. Alghafli, Khawla Abdulla, Andrew Jones, and Thomas Anthony Martin. "Forensic analysis of the Windows 7 registry." (2010).
2. “Background Activity Moderator Driver - Windows 10 Service - Batcmd.Com.” Batcmd, batcmd.com/windows/10/services/bam. Accessed 24 Dec. 2021.
3. Calder, Alan. "IT governance: A manager's guide to data security and ISO 27001/ISO 27002." (2008).
4. Carvey, Harlan. Windows forensic analysis DVD toolkit. Syngress, 2018.
5. Carvey, Harlan. "The Windows Registry as a forensic resource." Digital Investigation 2.3 (2005): 201-205.
6. Carvey, Harlan. Windows registry forensics: Advanced digital forensic analysis of the windows registry. Elsevier, 2011.
7. Carvey, Harlan. Windows forensic analysis DVD toolkit. Syngress, 2018.
8. Farmer, Derrick J., and V. Burlington. "A forensic analysis of the Windows registry." Champlain College Burlington, Vermont (2007).
9. Farmer, Derrick J., and V. Burlington. "A Windows registry quick reference: for the everyday examiner." Forensic Focus (2007): 1-14.
10. Greg-Lindsay. “What’s New in Windows 10, Version 1709 - What’s New in Windows.” Microsoft Docs, 19 Nov. 2021, docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1709#windows-analytics.
11. Microsoft Corporation, Windows registry information for advanced users, Redmond, Washington (support.microsoft.com/kb/256986), 2008.
12. “ROT13 Is Used in Windows? You’re Joking!” Didier Stevens, 24 July 2006, blog.didierstevens.com/2006/07/24/rot13-is-used-in-windows-you%E2%80%99re-joking.
13. Sikorski, Michael, and Andrew Honig. Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press, 2012.
14. Jwmsft. “KNOWNFOLDERID (Knownfolders.h) - Win32 Apps.” Microsoft Docs, 21 Aug. 2021, docs.microsoft.com/en-us/windows/win32/shell/knownfolderid.
15. Zhu, Yuandong, Pavel Gladyshev, and Joshua James. "Temporal analysis of Windows MRU registry keys." IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg, 2009.