**Process Explorer**

**Laura Dabelić, 003645771**

**Mentor: prof. Marin Golub**

**Akademska godina 2014/2015**

**Sadržaj**

1. Uvod ................................................................................................................................... 3
2. Grafičko sučelje .................................................................................................................. 4

2.1. Opis pojedinih opcija i detalji grafičkog sučelja ......................................................... 6

1. Detaljna analiza procesa ..................................................................................................... 13

3.1. TCP/IP .......................................................................................................................... 13

3.2. Security ........................................................................................................................ 14

3.3. Environment .................................................................................................................15

3.4. Strings .......................................................................................................................... 16

3.5. Image ............................................................................................................................17

3.6. Performance ................................................................................................................. 18

3.7. Performance Graph ...................................................................................................... 18

4. Primjeri korištenja Process Explorera za analizu zloćudnih programa .............................. 19

5. Zaključak ............................................................................................................................ 23

6. Literatura ............................................................................................................................ 24

**1. Uvod**

Process Explorer je besplatan program koji predstavlja nadograđenu i napredniju inačicu Windowsovog programa "Task Manager" te uz njegovu osnovnu funkcionalnost pruža i mnoge mogućnosti za prikupljanje i analizu informacija o procesima na korisničkom računalu. Razvio ga je Windows Sysinternals koji je dio Microsoftovog tima zaduženog za razvoj programske potpore namijenjene podešavanju, praćenju i otklanjanju problema Microsoftovog razvojnog okruženja. Moguće ga je pokrenuti na operacijskim sustavima od Windows XP nadalje.

Osim već spomenute mogućnosti analize procesa, Process Explorer također može poslužiti i za praćenje drugih problema operacijskog sustava pa se zbog toga koristi prilikom dinamičke analize zloćudnih programa. Neke od mogućnosti koje Process Explorer pruža su:

* Hijerarhijski pregled svih aktivnih procesa i njihovih svojstava
* Ispis svih dinamičkih knjižnica (Dynamic Link Library) koje je proces učitao
* Općenite informacije o sustavu
* Pokretanje, provjeravanje, zaustavljanje i ubijanje procesa
* Praćenje iskoristivosti procesora (CPU)
* Prikaz ikone i imena tvrtke proizvođača
* Postavljanje prioriteta procesa
* Prikaz korisničkih računa na sustavu
* Putanju slike procesa (image path) na disku
* Pregled rada Windows aplikacija

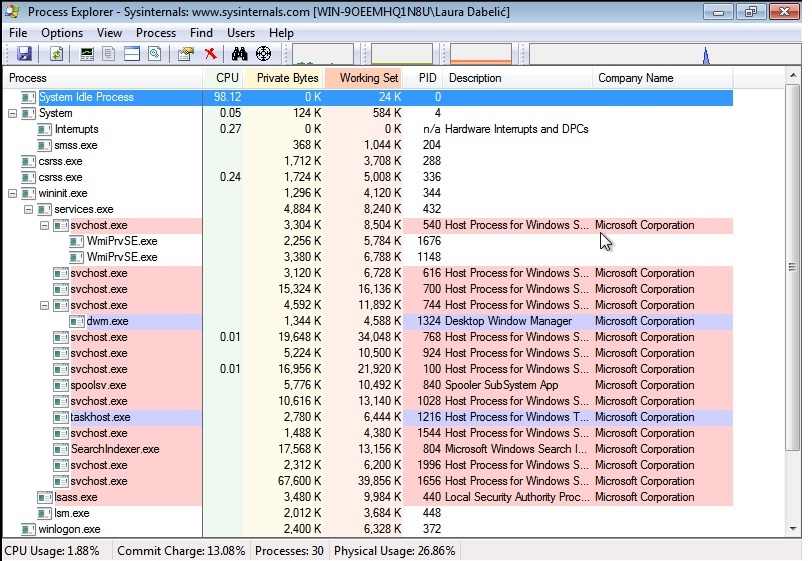
Moguće je podesiti da Process Explorer u potpunosti zamijeni Windows Task Manager opcijom *Replace Task Manager*. U tom slučaju, kada odaberemo opciju pokretanja Task Managera, umjesto njega će se pokrenuti Process Explorer. Ovo je globalna postavka sustava što znači da će se odraziti na sve korisnike operacijskog sustava. Ukoliko korisnik želi ponovno vratiti postavke da koristi Task Manager prilikom njegovog pokretanja, to može učiniti opcijom *Restore Task Manager*.

Process Explorer nije potrebno instalirati. Dovoljno je otići na stranicu <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>, preuzeti arhivirane datotke, te pokrenuti datoteku procexp.exe.

**2. Grafičko sučelje**

Izgled sučelja Process Explorera prikazan je na slici 2.1. Vidimo prikaz stablaste strukture procesa roditelja i njihove djece. Vide se odnosi roditelj-dijete. Sučelje se može podijeliti na stupce koji predstavljaju sljedeće cjeline:

* Process – prikazuje ime procesa
* CPU – koliko procesorskih resursa određeni proces koristi
* Private Bytes – prikazuje koliko byteova memorije je pojedini proces alocirao i ne može ih dijeliti sa drugim procesima
* Working Set – prikazuje količinu stranica memorije koje su iskoristile dretve procesa
* PID – identifikacijski broj pojedinog procesa
* Description – dodatni opis procesa
* Company Name – ime proizvođača programa kojemu odabrani proces pripada

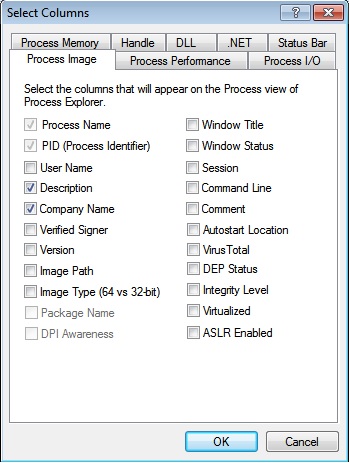


Slika 2.1. - Grafičko sučelje Process Explorera

Osim opisanih stupaca, sučelje sadrži i sljedeće dijelove:

* Meni – pokretanje akcija
* Alatna traka – za brzi pristup često korištenim opcijama i lakše snalaženje
* Statusna traka na dnu prozora – prikazuje dodatne informacije

Ovo su samo neke od opcija koje Process Explorer prikazuje prilikom prvog pokretanja. Međutim, može se omogućiti prikaz mnoštva dodatnih stupaca koji prikazuju još više korisnih informacija. U Meniu treba odabrati karticu *View* i opciju *Select Columns*. Nakon toga, otvorit će se dodatni prozor koji je prikazan na slici 2.2.

Slika 2.2 – prozor Select Columns

Prozor je podijeljen na više odjeljaka od kojih svaki predstavlja jednu kategoriju. Svaka kategorija nudi opcije za stupce koji se mogu prikazati tako da se ime pojedinog stupca označi kvačicom. Opis svake kategorije vidljiv je u tablici 2.1.

|  |  |
| --- | --- |
| **Kategorija** | **Opis kategorije** |
| Process Image | Općenite informacije o slici procesa kao što su ime korisnika, putanju slike procesa na disku (image path), ime tvrtke ili lokacija automatskog pokretanja. |
| Process Performance | Informacije o izvođenju procesora kao što su iskoristivost procesora i njezina povijest, početak procesa, dretve koje proces koristi, promjena konteksta i osnovni prioritet. |
| Process I/O | Informacije o operacijama čitanja i pisanja koje je proces izveo te povijest svih tih operacija. |
| Process Memory | Informacije o količini memorije koju je proces zauzeo i način na koji je memorija bila korištena |
| Handle | Stupci koji prikazuju informacije o *handle*ovima |
| DLL | Informacije o dinamičkim knjižnicama |
| .NET | Informacije vezane za .NET razvojno okruženje |
| Status Bar | Informacije prikazane u statusnoj traci na samom dnu prozora grafičkog sučelja |

Tablica 2.1. - Kategorije u prozoru Select Columns

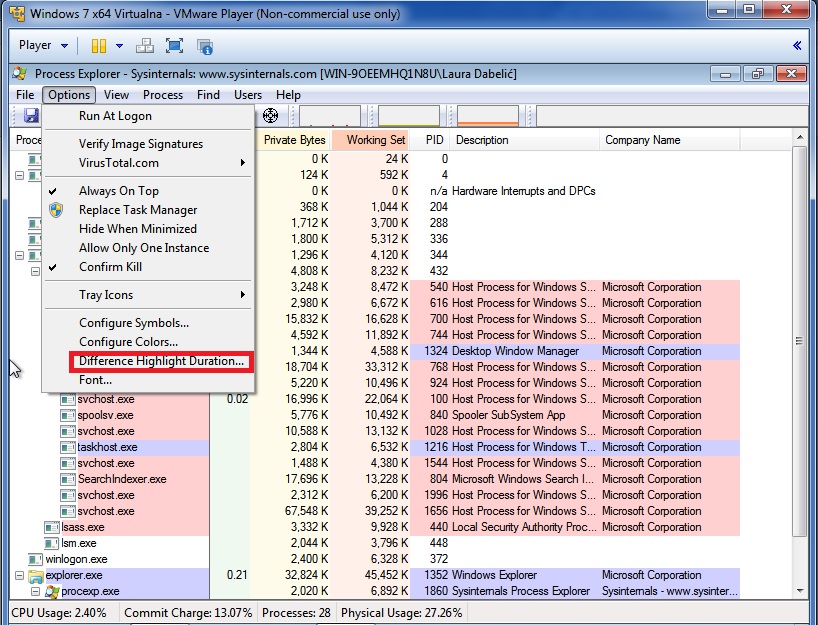
**2.1 Opis pojedinih opcija i detalji grafičkog sučelja**

Svake sekunde informacije koje vidimo o procesima se mijenjaju kako neki procesi odumiru i završavaju se, a novi tek počinju i pokreću se. Vidimo da su pojedini dijelovi ispisa označeni različitim bojama. Značenje svake boje opisano je sljedećom tablicom:

|  |  |
| --- | --- |
| **Boja** | **Značenje u grafičkom sučelju** |
| Ružičasta | Prikazuje usluge |
| Plava | Prikazuje procese |
| Zelena | Novi procesi koji su tek započeli |
| Crvena | Završeni procesi koji su prekinuti |
| Ljubičasta | Označava da se radi o prisutnosti pakiranog koda |

Tablica 2.2. - Značenje pojedinih boja u grafičkom sučelju Process Explorera

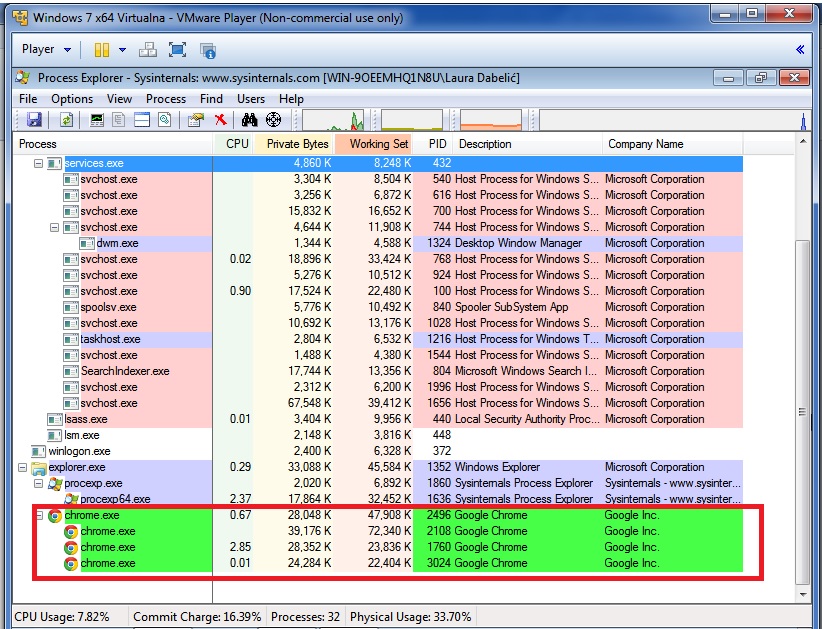
Kod prvog pokretanja Process Explorera, zelena i crvena boja procesa koji se pokreću i odumiru se ne vidi jer je trajanje njihovog prikaza podešeno na samo 1 sekundu. Da bismo vidjeli kada se pojedini proces pokrenuo i kada se prekinuo, treba podesiti trajanje prikaza odabirom kartice Options u Meniu i odabirom opcije *Difference Higlight Duration* kako je prikazano na slici 2.3. Otvorit će se dodatni prozor u kojemu će se moći podesiti vrijeme prikaza vremena koja želimo vidjeti. Preporučljivo je podesiti vrijeme prikaza na 5 – 10 sekundi.



Slika 2.3. - Podešenje vremena prikaza početka i odumiranja procesa

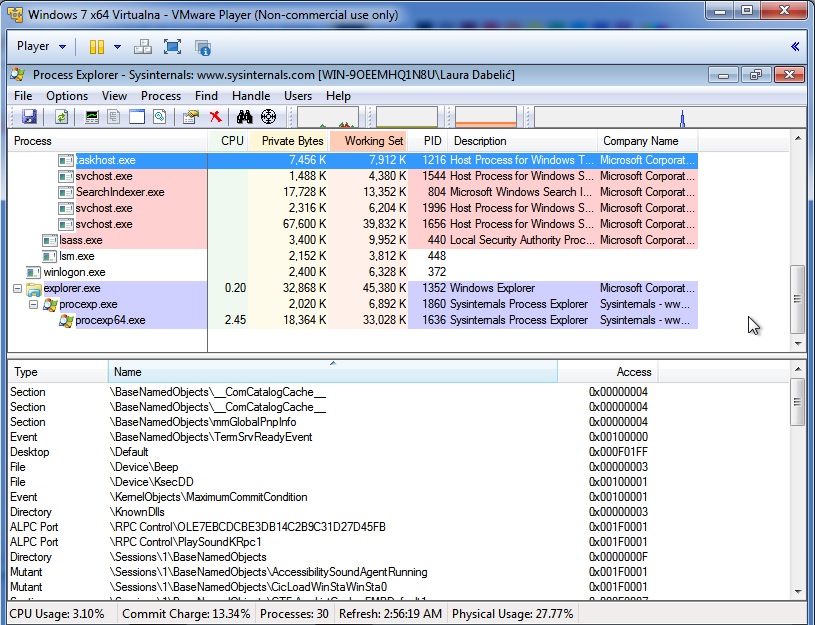
Ako želimo da Process Explorer bude stalno otvoren kao prvi prozor koji vidimo dok otvaramo programe čije procese analiziramo, potrebno je odabrati opciju *Always On Top* koja se također nalazi u kartici Options i također je vidljiva na slici 2.3 i označena kvačicom. Sada Process Explorer neće otići “u pozadinu” kada kliknemo na neki drugi program koji pokrećemo i imat ćemo bolji pregled nad svim aktivnostima promatranih procesa.

Sada kada smo namjestili vidljivost trajanja procesa, možemo za primjer pokrenuti internetski preglednik Google Chrome i vidjeti kako su njegovi procesi prikazani u sučelju Process Explorera zelenom bojom kako prikazuje slika 2.4.



Slika 2.4 – Prikaz početka procesa nakon pokretanja internetskog preglednika Google Chrome

U kartici *View* možemo odabrati opciju *Show Lower Pane*. Tada će nam se grafičko sučelje podijeliti na dva prozora. U gornjem prozoru vidjet ćemo sve što smo vidjeli i dosad, a u donjem prozoru prikazat će nam se popis svih dinamičkih knjižnica koje je određeni proces učitao u memoriju. U gornjem prozoru treba kliknuti na proces koji želimo promatrati. Rezultat takvog pregleda procesa taskhost.exe prikazan je na slici 2.5



Slika 2.5 – Prikaz svih učitanih dinamičkih knjižnica procesa taskhost.exe

Meni osim gore spomenutih opcija nudi još i sljedeće opcije:

* **File** – nudi opcije pokretanja kao administrator ili kao ograničeni korisnik (Limited User). Preporuča se odabrati opciju *Run as Administrator* jer je tako korisniku dostupno više opcija. Također postoje opcija snimanja trenutnog stanja procesa i prikaz detalja za sve procese
* **Edit** – nudi opcije pokretanja čim se korisnik prijavi na sustav, provjere potpisa slike (Image Signatures), provjera postoji li datoteka ili proces u bazi podataka na stranici VirusTotal.com, opciju da je Process Explorer uvijek na vrhu, promjena fonta, zamjena Task Managera i podešavanje konfiguracije programa.
* **View –** nudi odabir stupaca koje želimo prikazati, prikazivanje ili sakrivanje prozora sa dinamičkim knjižnicama te vizualnu organizaciju sučelja
* **Process** – nudi opcije postavljanje prioriteta procesa, ubijanja pojedinačnog procesa ili cijelog njegovog stabla, zaustavljanje i ponovno pokretanje procesa i provjera stranice VirusTotal
* **Find** – nudi opciju pronalaženja dinamičke knjižnice i apstraktnih referenci prema resursima (handle)
* **Handle** – *handle*a. Zahtijeva ovlasti administratora
* **Users –** prikazuje popis trenutno aktivnih korisnika
* **Help** – nudi pomoć pri korištenju alata i dodatne informacije

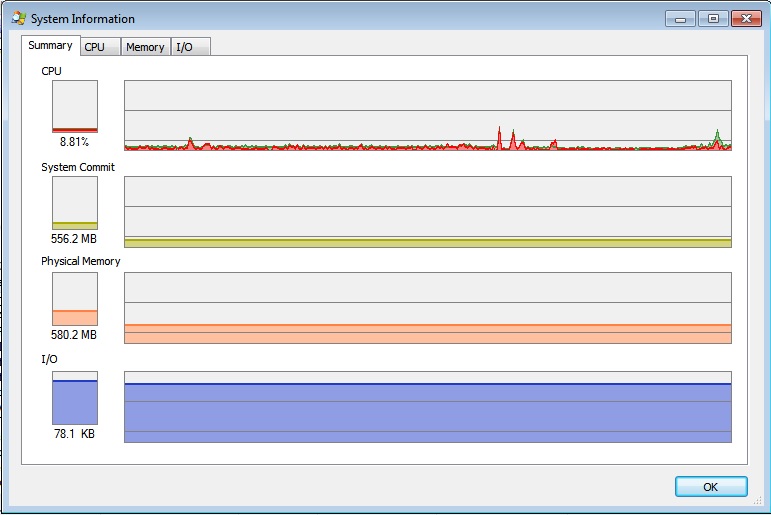
Ako nekom od alata želimo brzo pristupiti, za to nam može poslužiti alatna traka. Funkcionalnosti koje alatna traka pruža vidljive su u tablici 2.3.

|  |  |  |
| --- | --- | --- |
| **Ikona** | **Ime ikone** **i prečac** | **Opis** |
|  | Save (Ctrl + S) | Omogućava spremanje trenutnog stanja procesa i ispisa dinamičkih knjižnica ako je prikazan |
|  | Refresh Now (F5) | Ručno osvježavanje ispisa trenutnog stanja sustava |
|  | System Information (Ctrl + I) | Otvara prozor sa grafovima (Summary, CPU, Memory i I/O) |
|  | Show Process Tree | Omogućava povratak na izvorni ispis stabla procesa ako smo ručno promijenili redosljed ispisa procesa |
|  | Hide Lower Pane | Omogućava prikaz ili sakrivanje donjeg prozora sa ispisom dinamičkih knjižnica |
|  | Properties | Omogućava ispis dodatnih informacija o pojedinom procesu |
|  | Kill Process/Close Handles | Ubija proces ili zatvara *handle*ove |
|  | Find Handle or DLL (Ctrl + F) | Pronalazi *handle* |
|  | Find Window's Process | Omogućava prikaz procesa koji je pokrenuo određeni prozor operativnog sustava. Nakon klika na ikonu, prikazani znak se postavi na prozor za koji nas zanima kojem procesu pripada. |

Tablica 2.3. – Funkcionalnosti alatne trake

U tablici 2.3. možemo vidjeti da ikona *System Information* otvara prozor sa grafovima. Moguće je prikazati četiri grafa kako je već nabrojano: Summary, CPU, Memory i I/O. U nastavku je dan prikaz svakog grafa i kratki opis.

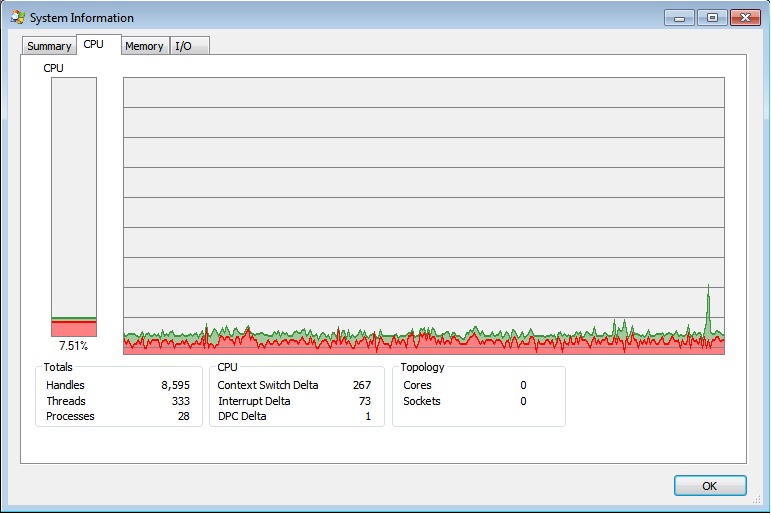
Kad kliknemo ikonu *System Information* prvo će nam se otvoriti opcija Summary koji prikazuje sva četiri moguća grafa na jednom mjestu. Klikom na preostale tri opcije možemo vidjeti svaki od tih grafova detaljnije prikazan i sa više informacija. Izgled opcije *Summary* prikazan je na slici 2.6.



Slika 2.6. - System Information prozor sa opcijom Summary

Opcija CPU u prozoru *System Information* otvara nam prozor sa grafičkim prikazom iskoristivosti procesora kao što je prikazano na slici 2.7. Ispod grafa vidimo sljedeće informacije o pocesorskim aktivnostima:

* Handles – handleovi
* Threads – broj aktivnih dretvi
* Processes – broj trenutno aktivnih procesa
* Context Switch Delta – podaci o promjeni konteksta, to jest promjene koje su se dogodile između dva izvođenja koda
* Interrupt Delta – podaci o sklopovskim prekidima
* DPC Delta – podaci o DPC-ovima (Deferred Procedure Call)
* Cores – podaci o jezgrama procesora
* Sockets – podaci o priključcima



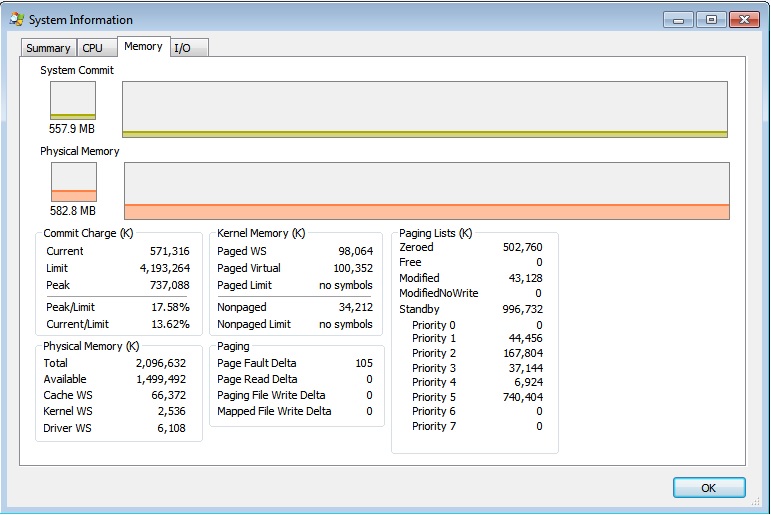
Slika 2.7 – System Information prozor sa opcijom CPU

Opcija *Memory* u prozoru *System Information* otvara nam prozor koji je prikazan na slici 2.8. Možemo vidjeti dva grafa:

* System Commit – prikazuje količinu virtualne memorije alociranu svim procesima u sustavu.
* Physical Memory – prikazuje količinu fizičke memorije sustava

Ispod grafova možemo vidjeti informacije o memoriji grupirane u nekoliko podkategorija:

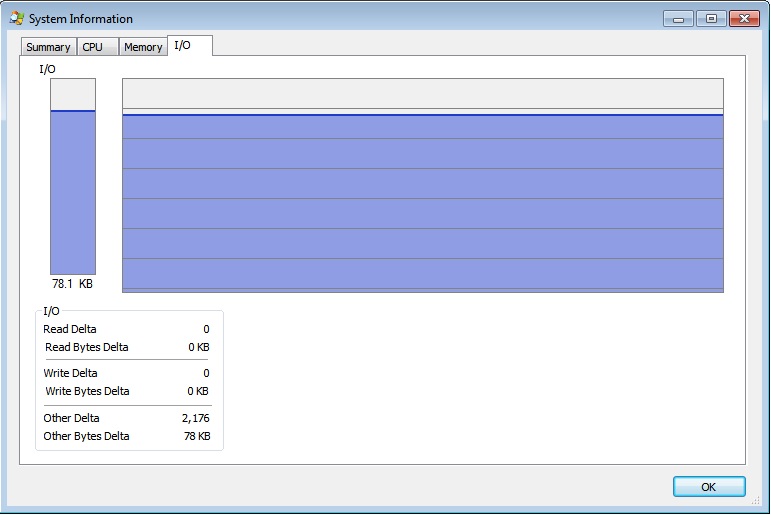
* Commit Charge – količina adresnog prostora dostupna straničenjem. Prikazuje i granicu adresnog prostora koja je izražena kao suma trenutnih straničenih datoteka i slobodne fizičke memorije za straničenje te najveću vrijednost (Peak).
* Physical Memory – detalji o količini fizičke memorije
* Kernel Memory – zajedno sa sljedeće dvije opcije daje informacije o straničenju
* Paging
* Paging Lists



Slika 2.8. - System Information prozor sa opcijom Memory

Opcija *I/O* u prozoru *System Information* otvara nam prozor koji je prikazan na slici 2.9. Vidimo graf u obliku plave crte koji prikazuje ukupni promet unosa i ispisa na sustavu. To je suma operacija unosa i ispisa svih procesa između dva osvježavanja prikaza. Ako prijeđemo mišem preko grafa ispisat će nam se ime procesa koji izvodi najviše operacija unosa i ispisa. Ispod grafa, nalaze se dodatne informacije o operacijama unosa i ispisa:

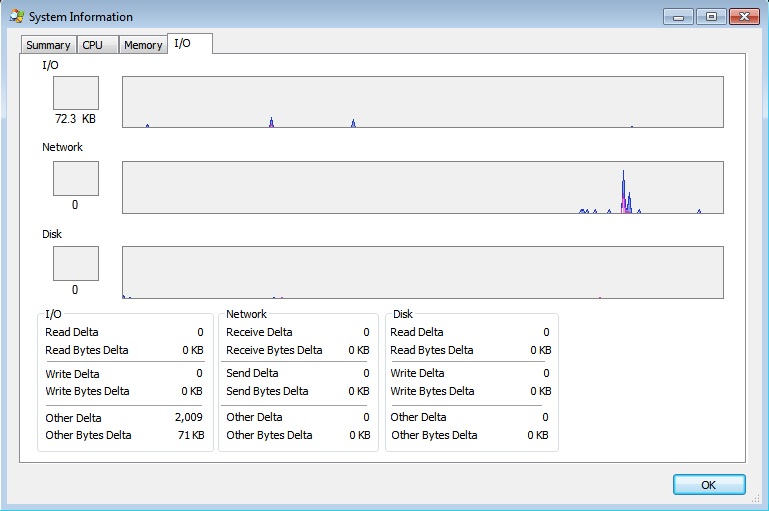
* Read Delta
* Read Bytes Delta
* Write Delta
* Write Bytes Delta
* Other Delta
* Other Bytes Delta



Slika 2.9 – System Information prozor sa opcijom I/O

Važno je napomenuti da će se ovi prikazi vidjeti ako se Process Explorer pokrene kao obični korisnik što ima ograničenja. Ukoliko se pri pokretanju Process Explorera odabere opcija *Run as Administrator*, grafovi će prikazivati i neke dodatne detalje kao što su podaci o aktivnostima mreže i diska.

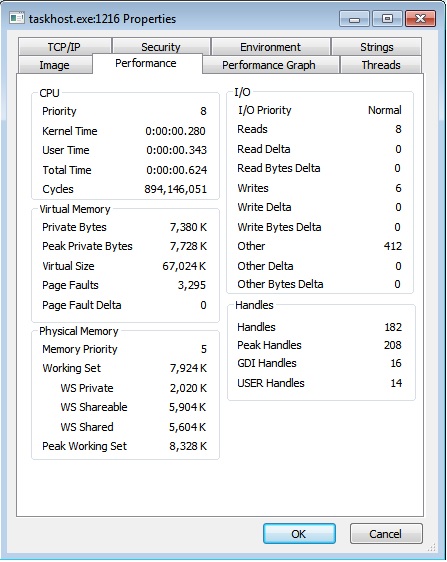
Stoga je preporučljivo pokretati Process Explorer kao administrator da bi se moglo iskoristiti njegovu punu funkcionalnost. Primjer dodatnih detalja najbolje se vidi ako kao administrator pogledamo prikaz System Information prozora što je prikazano na slici 2.10.



Slika 2.10. - System Information prozor pokrenut kao administrator

**3. Detaljna analiza procesa**

Desnim klikom miša na proizvoljno odabrani proces, primjerice taskhost.exe i odabirom opcije *Properties* otvorit će nam se novi prozor prikazan na slici 3.1.



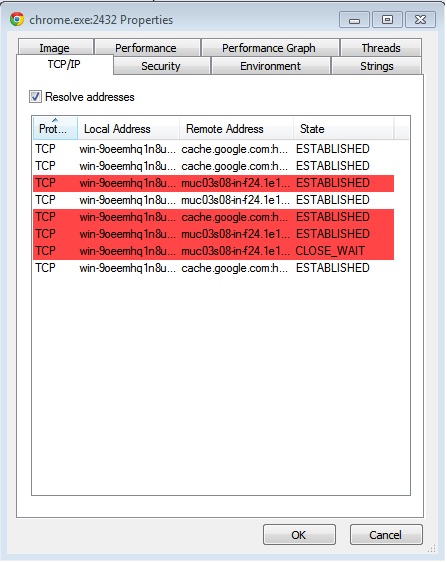
Slika 3.1. - Prozor Properties procesa taskhost.exe sa prikazom opcije Performance

Prozor je podijeljen na 8 logičkih cjelina:

* TCP/IP
* Security
* Environment
* Strings
* Image
* Performance
* Performance Graph
* Threads

**3.1 TCP/IP**

Programi koji koriste Internet kao na primjer internetski preglednici imat će nekoliko veza ostvarenih putem TCP/IP protokola. Cjelina TCP/IP u prozoru *Properties* prikazuje aktivnost TCP/IP protokola i osvježava se u stvarnom vremenu tako da vidimo zelenom bojom označene veze koje su se tek uspostavile, a crvenom one koje su se prekinule. Ako otvorimo internetski preglednik Google Chrome i otvorimo TCP/IP prozor za proces chrome.exe, rezultat će biti sličan prikazu sa slike 3.2.



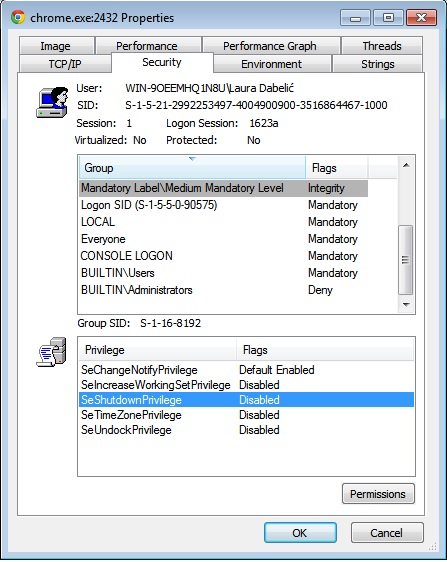
Slika 3.2 – TCP/IP aktivnost procesa chrome.exe

Kod analize zloćudnih programa, ova opcija nam može biti korisna kod praćenja internetske aktivnosti zloćudnog procesa i adresa s kojima proces putem Interneta komunicira.

**3.2 Security**

Cjelina *Security* prikazana je na slici 3.3. U prvom dijelu prozora vidimo informacije o korisnicima kao što su njihove prijave na sustav i razine ovlasti. Donji dio prozora prikazuje privilegije, to jest mogućnosti koje proces posjeduje a drugi procesi ih nemaju ovisno o stanju zastavice (desni stupac Flags). Ako je u stupcu Flags zastavica za neku privilegiju postavljena na Enabled, proces će moći izvoditi akciju definiranu tom zastavicom. Neke privilegija su:

* SeShutdownPrivilege – mogućnost isključivanja računala
* SeTimeZonePrivilege – mogućnost promjene vremenske zone
* SeIncreaseWorkingSetPrivilege – mogućnost alociranja većeg dijela memorije
* SeChangeNotifyPrivilege – mogućnost obavijesti o promjeni nad datotekama
* SeCreatePermanentPrivilege – mogućnost stvaranja trajnog objekta
* SeLockMemoryPrivilege – mogućnost zaključavanja fizičkih stranica u memoriji
* SeMachineAccountPrivilege – mogućnost stvaranja korisničkog računa na sustavu

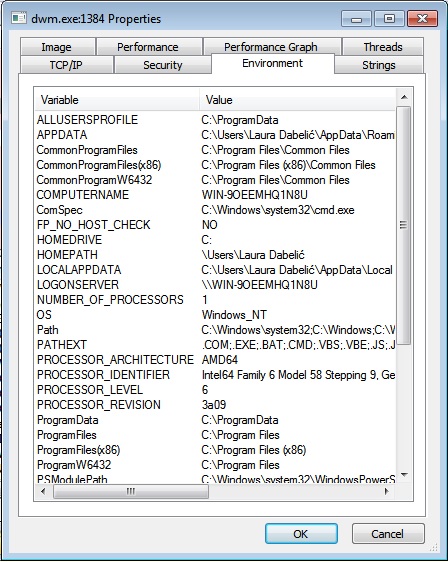


Slika 3.3 – Sigurnosne informacije

**3.3. Environment**

Cjelina *Environment* prikazana je na slici 3.4. Vidimo ispis varijabli okoline (environment variables) i njihove vrijednosti. Varijable okoline mogu utjecati na ponašanje procesa na računalu i dio su okoline u kojoj se proces pokreće. Svaki proces ima svoj skup varijabli okoline. Kad se proces stvori, on nasljeđuje “preslikanu” okolinu svoga roditelja osim promjena koje je proces-roditelj napravio prilikom svaranja procesa-djeteta. Neki primjeri varijabli okoline su:

* PATH – popis putanja na disku
* HOME – označavaju korisnikov glavni direktorij (home directory) na sustavu
* TERM – označava vrstu terminala koji se koristi na operacijskom sustavu
* MAIL – koristi se za nalaženje korisnikove elektroničke pošte
* TEMP – lokacija na koju proces može spremati privremene datoteke
* USERNAME – ime korisnika trenutno prijavljenog na sustav
* OS – označava operacijski sustav



Slika 3.4 – prikaz varijabli okoline

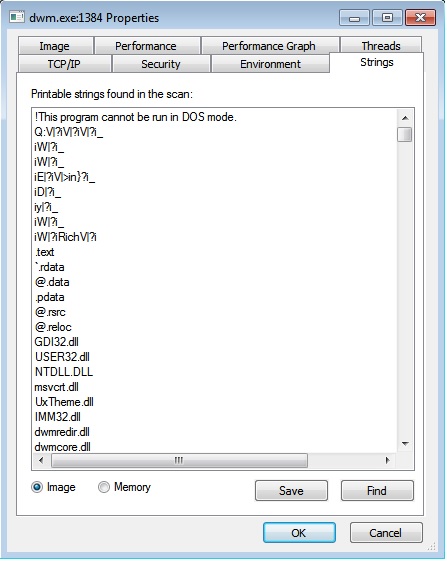
**3.4. Strings**

Cjelina *Strings* prikazana je na slici 3.5. Prikazuje ispis svih znakovnih nizova duljine 3 znaka i više. Ispod prikaza vidimo dvije moguće opcije prikaza znakovnih nizova: *Image* i *Memory*.

Opcija *Image* prikazuje znakovne nizove pročitane iz slike procesa na disku (process image file), dok opcija *Memory* prikazuje znakovne nizove pročitane iz dijela memorije u kojem je slika procesa na disku spremljena.

Znakovni nizovi na disku mogu se razlikovati od znakovnih nizova iz memorije i pomoću ove opcije to možemo provjeriti tako da usporedimo ispise znakovnih nizova na disku i iz memorije. Ako se ispisi znakovnih nizova jako razlikuju, možemo posumnjati da je korištena metoda zamjene procesa (process replacement) koju često koriste zloćudni programi kako bi prikrili svoju aktivnost. Nakon izvođenja ove metode, zloćudni program stječe svojstva legitimnog procesa kojeg zamjenjuje i zbog toga izgleda kao potvrđeni, originalni program. Međutim, ova metoda ostavlja trag u obliku različitih ispisa znakovnih nizova u memoriji i na disku.

Također, ako vidimo jako malo znakovnih nizova u ispisu, možemo posumnjati da se radi o pakiranom programu. Pakiranje je metoda koju koriste maliciozni programi kako bi ih se teže otkrilo. Nakon rasprakiravanja možemo dobiti ispis svih znakovnih nizova koji će nam koristiti u daljnoj analizi.



Slika 3.5. - ispis znakovnih nizova

**3.5. Image**

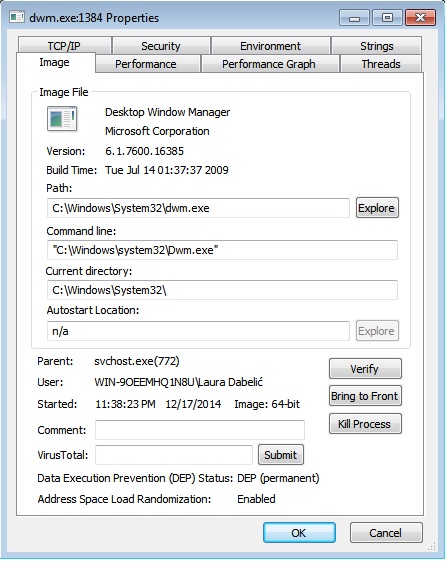
Cjelina *Image* prikazana je na slici 3.6. Vidimo informacije kao što su putanja na disku do procesa, vrijeme kad je proces započeo, koja komandna linija je bila iskorištena kako bi se proces pokrenuo, korisnika na sustavu i proces-roditelj.

Gumbom *Verify* možemo provjeriti da li slika procesa na disku sadrži Microsoftov potpis. Microsoft koristi digitalne potpise za većinu svojih programa. Ovom opcijom možemo provjeriti je li proces potvrđen od strane Microsofta. Moguće su tri opcije koje Process Explorer može ispisati:

* Trusted – slika sadrži potpis
* Unsigned – slika ne sadrži potpis
* Not Verified – slika još nije bila provjerena

Zloćudni programi često zamjenjuju datoteke na disku svojima i na ovaj način možemo to provjeriti. Nedostatak *Verify* opcije jest u tome što ona provjerava samo da li je promatrana slika na disku ali na i u memoriji.

Kao što je već rečeno u odjeljku 3.4, zloćudni program može koristiti metodu zamjene procesa kako bi se predstavio kao potvrđeni program. Stoga se nakon ove metode provjere preporuča provjeriti proces metodom usporedbe znakovnih nizova na disku i u memoriji kako je opisano u odjeljku 3.4.



Slika 3.6. - podaci o slici procesa na disku

**3.6. Performance**

Cjelina *Performance* prikazana je na slici 3.1. Prikazuje informacije o izvođenjima procesora i memorije kao što su izvodivost procesora te količina virtualne i fizičke memorije. Prikaz sadrži nekoliko podkategorija:

* CPU
* Virtual Memory
* Physical Memory
* I/O
* Handles

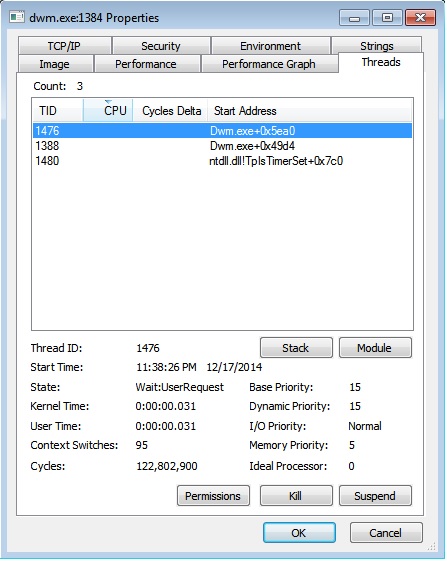
**3.7. Performance Graph**

Daje grafički prikaz stanja procesora i memorije, nešto sažetiji nego prikaz koji daje *System Information* opisan u odjeljku 2.1.

**3.8. Threads**

Cjelina *Threads* prikazana je na slici 3.7. Vidimo popis dretvi u procesima. Vidimo početnu adresu svake dretve koju nam daje Windows Symbol Engine i broj dretve (Thread ID). Ispod ispisa dretvi možemo vidjeti dodatne informacije o svakoj dretvi ako kliknemo na nju:

* Thread ID – broj dretve
* Start Time – vrijeme kad je dretva započela s radom
* State – status dretve
* Kernel time – vrijeme jezgre operacijskog sustava
* User time – vrijeme korisnika
* Context switches – broj zamjena konteksta
* Cycles – broj ciklusa dretve
* Base Priority – početni prioritet dretve
* Dynamic Priority – dinamički prioritet dretve. U početku je isti kao i bazni prioritet. Operativni sustav može mijenjati dinamički prioritet kako bi osigurao da sve dretve dobivaju jednako procesorskog vremena
* I/O priority – prioritet kod unosa i ispisa.
* Memory priority – može poprimiti vrijenost 1-5. Služi kao pomoćna informacija operacijskom sustavu kod raspodjele memorije. Broj 1 označava najniži prioritet, a broj 5 najviši koji je ujedno i standardni prioritet za sve procese i dretve u sustavu.

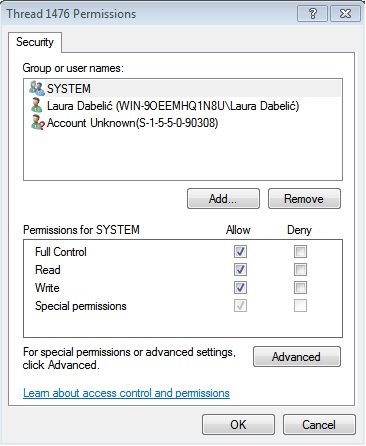


Slika 3.7. popis dretvi u procesima

Gumbima *Kill* i *Suspend* možemo ubiti ili zaustaviti označenu dretvu. Gumbi *Stack* i *Permissions* otvaraju dodatne prozore koji pružaju informacije o stanju stoga i dopuštenjima određenih korisnika da izvode određene akcije.

**4. Primjeri korištenja Process Explorera za analizu zloćudnih programa**

Za analizu zloćudnih programa često nam dobro može doći gumb Permissions. Prozor koji se otvara nakon što kliknemo na gumb prikazan je na slici 4.1.



Slika 4.1. - prozor Permissions

Primjerice, otkrili smo zloćudni program čiji proces se ne može ubiti jer ima nekoliko pomoćnih procesa koji ga uvijek vrate. Zloćudni program pokreće se u isto vrijeme kad i operacijski sustav. Opcije koje nam nudi prozor Permissions mogu nam omogućiti da zloćudnom programu onemogućimo rad prilikom sljedećeg poktetanja sustava.

Kao što vidimo na slici 4.1, prozor Permissions podijeljen je na dva podprozora. Gornji prozor prikazuje sustav i sve korisnike, a donji popis dopuštenih akcija. Ako za proces zloćudnog programa zabranimo pristup svim korisnicima uključujući i operacijski sustav, prilikom idućeg pokretanja operacijskog sustava zloćudni program se uopće neće uspjeti pokrenuti.

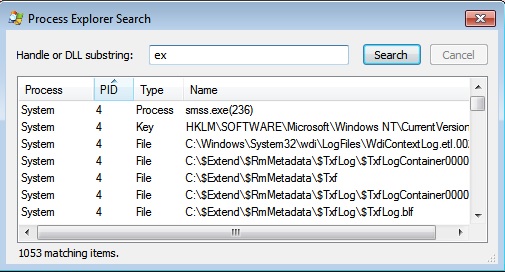
Postoji i prečac preko komandne linije kojim možemo izvesti ovo isto. Potrebno je otvoriti komandnu liniju, pozicionirati se u direktorij gdje smo pomoću Process Explorera locirali da se nalazi zloćudni program i utipkati sljedeću naredbu:

* caecls imeZloćudnogPrograma.ekstenzija ID Everyone

Ova imeZloćudnogPrograma vidjet ćemo u Process Exploreru kao i ekstenziju. Everyone označava da će pristup apsolutno svima biti zabranjen (svim korisnicima i operacijskom sustavu).

Metoda koja se često koristi u analizi zloćudnih programa jest provjera dinamičkih knjižnica (DLL). U meniu odaberemo karticu *Find* i potom opciju *Find Handle or DLL.* Otvorit će nam se prozor koji je prikazan na slici 4.1.

U prozoru vidimo polje *Find Handle or DLL substring* u koje upišemo ime ili dio imena tražene dinamičke knjižnice ili *handle*a. U podprozor ispod ispisat će nam se popis svih procesa koji u imenu sadrže traženi pojam. To su procesi koji koriste traženu dinamičku knjižnicu.



Slika 4.1. - prozor za traženje dinamičkih knjižnica

Process Explorer također može poslužiti i za analizu zaraženih, malicioznih dokumenata kao što su PDF ili Word dokumenti. Prvo otvorimo Process Explorer, a potom otvorimo sumnjivi dokument. Ako dokument nakon svog otvaranja pokrene neke dodatne procese, možemo ih analizirati pomoću Process Explorera i locirati zloćudni program na disku.

Proces dinamičke analize opisan je bez konkretnih primjera jer nije bilo moguće zaraziti virtualni stroj i pogledati ponašanje zloćudnog programa na simuliranom operacijskom sustavu.

**5. Zaključak**

Process Explorer ima široku upotrebu u otkrivanju i otklanjanju problema prouzročenih od strane samog sustava i od malicioznih programa. Mnoštvo opcija koje pruža mogu pokriti širok spektar problema. Unatoč tome, potrebno je neko vrijeme da bi se sve opcije istražile i upoznale kao i poznavanje stručnih pojmova vezanih uz operacijske sustave. Prije korištenja Process Explorera preporuča se ovladati tim područjem računarstva. Stoga je Process Explorer namijenjen naprednijim korisnicima i korisnicima koji se bave analizom zloćudnih programa.

**6. Literatura**

[1] Process Explorer: <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

[2] Fakultet elektrotehnike i računarstva; Radovi iz područja računalne sigurnosti; 2014;

<http://os2.zemris.fer.hr/index.php?show=start>

[3] Michael Sikorski; Andrew Honig. Practical Malware Analysis: The Hands-On GuideTo Dissecting Malicious Software. San Francisco: no starch press, 2012