



Tusi Paleon - Malware Forensic Tool v1.0b

İstifadəçi Təlimatı

**Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti – Kompüter
İnsidentlərinə qarşı Mübarizə Mərkəzi – Malware Research Lab**

11 Aprel 2023

Mündəricat

1	Giriş.....	5
1.1	Laboratoriya haqqında.....	6
2	Tusi Paleon	6
2.1	Tələblər.....	6
2.2	Hədəf sistemdə quraşdırılması və silinməsi.....	7
2.3	İşə salınma prosesi.....	7
3	Məlumat bazası strukturu və cədvəllər	8
3.1	Cədvəllər	8
3.1.1	“Case” cədvəli və strukturu	8
3.1.2	“Processes” cədvəli və strukturu	9
3.1.3	“Services” cədvəli və strukturu.....	10
3.1.4	“Drivers” cədvəli və strukturu	10
3.1.5	“Tasks” cədvəli və strukturu	11
3.1.6	“Users” cədvəli və strukturu.....	11
3.1.7	“Windows” cədvəli və strukturu	11
3.1.8	“Disks” cədvəli və strukturu	11
3.1.9	“Autorun” cədvəli və strukturu	12
3.10.1	“Evt_Defender1116” cədvəli və strukturu.....	12
3.1.11	“ImageFileExecutions” cədvəli və strukturu	13
3.1.12	“Programs” cədvəli və strukturu	13
3.1.13	“IPConfig” cədvəli və strukturu	13
3.1.14	“DNSCache” cədvəli və strukturu	13
3.1.15	“Hosts” cədvəli və strukturu.....	14
3.1.16	“Firewall” cədvəli və strukturu	14
3.1.17	“Shares” cədvəli və strukturu.....	14
3.1.18	“IPRoute” cədvəli və struktur	14
3.1.19	“TCPTTable” cədvəli və strukturu	15

3.1.20	“UDPTable” cədvəli və strukturu	15
3.1.21	“ARPTable” cədvəli və strukturu.....	15
3.1.22	“System” cədvəli və strukturu.....	15
3.1.23	“Firefox tablosu” və strukturu.....	16
3.1.24	“Chrome” cədvəli və strukturu.....	16
3.1.25	“Edge” cədvəli və strukturu	17
3.1.26	“Opera” cədvəli və strukturu	17
3.1.27	“Run” cədvəli və strukturu	17
3.1.28	“Prefetch” cədvəli və strukturu.....	17
3.1.29	“Evt_UsrLogon_4624”	18

1 Giriş

Təcrübələrimiz əsasında kiberinsidentlər zamanı qarşılaşdığımız ən önəmli problemlərdən biri insidentin baş verdiyi əməliyyat sistemində zərərvericini aşkarlamaq üçün məlumat toplamağa çalışarkən istifadə etdiyimiz müxtəlif alətlər və yaşadığımız vaxt itkisidir. Belə ki, istifadə edilən müxtəlif alətlərin köməkliyi ilə sistem məlumatlarını toplamaq, onların təhlilini aparmaq, nəticə əldə etmək və əldə olunan nəticəni qarşı tərəfə (zərərçəkənə) raport etmək olduqca zəhmətli və vaxt tələb edən bir prosesidir. Bundan əlavə olaraq, bəzən hər hansı məlumatı toplamaq istəyərkən eyni anda bir neçə alətin dəstəyini almaq müəyyən mənada çətinliklər yarada bilər. Laboratoriya olaraq məhz bu təcrübələrimizdən faydalanaraq bu tip insident araşdırmaları zamanı effektivliyi qoruyub saxlamaq məqsədi ilə "Tusi Paleon" (bundan sonra Paleon) adını verdiyimiz aləti hazırladıq. Əsas üstünlüyü kiberinsident zamanı tək bir alətin köməkliyi ilə zərərverici proqram izlərini daşıya biləcək potensial sistem artefaktlarını toplayaraq vahid baza içərisində saxlaya bilməsi (şifrələnmiş və sıxışdırılmış formatda) və bu əməliyyat zamanı vaxt itkisini minimuma endirə bilməsidir. Alətin bir digər müsbət tərəfi isə toplanan sistem artefaktlarının həcmnin ənənəvi ekspertiza (forensics) alətlərinin topladığı məlumat həcmindən daha az olmasıdır. Çünki ənənəvi ekspertiza alətləri sistem məlumatlarını sərt disk və əməli yaddaşın bütünlüklə ehtiyat nüsxəsini çıxarmaqla və ya bütünlüklə təhlil etməklə toplayırlar. Bu tip metodlar günümüzdə hələ də effektiv olaraq istifadə edilsə də, sərt disk və əməli yaddaş həcmələrinin artması insident araşdırması zamanı əksər hallarda lazım olduğundan daha çox məlumat həcmi yaradır. Bundan əlavə olaraq bu tip məlumatları toplayarkən olduqca uzun vaxt itkisi yaşanır. Sözügedən problemləri və xüsusilə zərərvericilərin artan dinamikasını nəzərə almaqla yeni məhsulların hazırlanması aktual məsələ olmuşdur. Paleon sərt diski və əməli yaddaşı bütünlüklə təhlil etmədən real vaxt rejimində sistem məlumatlarını toplayır. Daha sonra isə zərərverici proqram analitiki toplanan xam məlumat üzərində araşdırma apararaq zərərverici haqqında informasiya əldə etməyə çalışır.

Niyə məhz zərərverici ekspertizası?

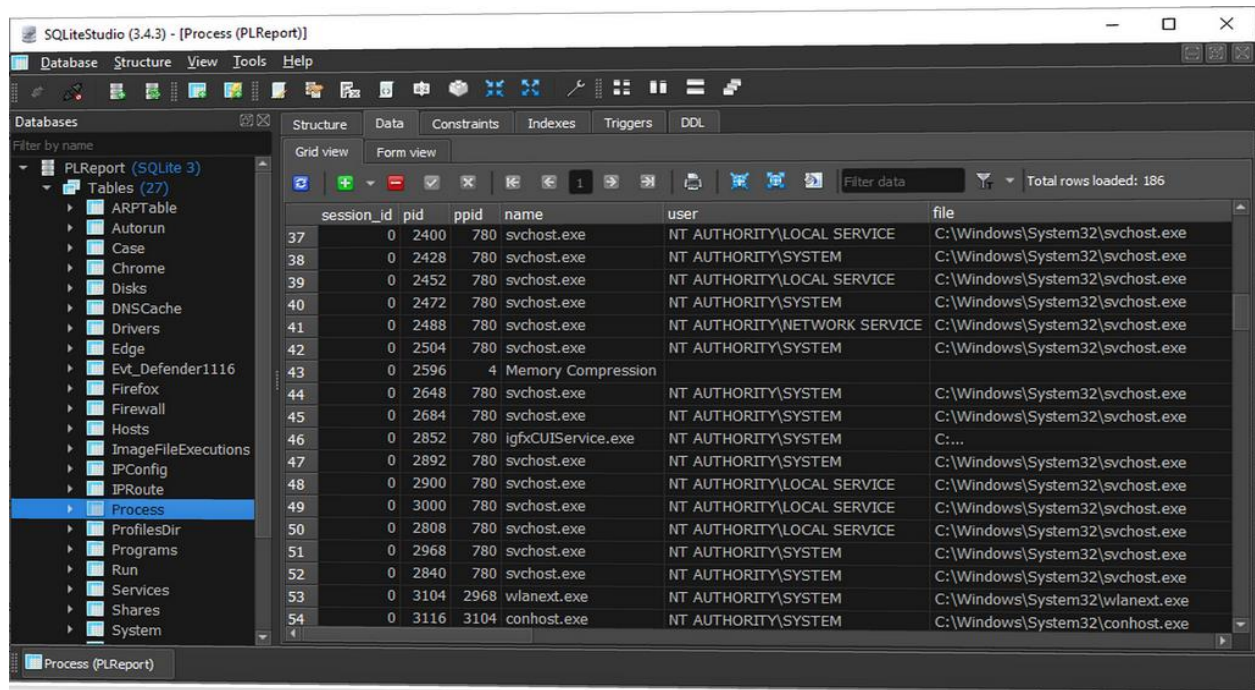
Paleonu "malware forensics" aləti adlandırmağımızın ən önəmli səbəbi isə onun standart kiberekspertiza proqram təminatlarından ayıran əsas fərqi məhz zərərverici ekspertizasına fokuslanmasıdır. Yəni Paleon rəqəmsal ekspertiza (**digital forensics**) aləti olaraq deyil, zərərverici proqram təminatlarına qarşı istifadə edilmək məqsədilə hazırlanmışdır.

1.1 Laboratoriya haqqında

Laboratoriya “Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi” - nin nəzdində, zərərli proqram təminatlarının analizi və onların tətqiqatı ilə məşğul olan mütəxəssilər tərəfindən yaradılmışdır. Əsas məqsədi Azərbaycan Respublikasının dövlət orqanlarını, kritik informasiya infrastrukturunu obyektlərini hədəf alan zərərli proqram təminatlarının analizi, müşahidəsi, tətqiqatı, habelə istifadəçilərin maarifləndirilməsi və bu sahədə yeni fəaliyyətə başlayan şəxsləri ilkin analiz vasitələri ilə təmin edərək sahənin inkişafına dəstək verməkdir.

2 Tusi Paleon

Giriş bölməsində qeyd edildiyi kimi Paleon-un əsas məqsədi zərərverici analitikini minimum vaxt itkisi ilə hədəf sistemdə zərərvericini aşkarlaması üçün ona aid izləri daşıya biləcək məlumatlar ilə təmin etməsidir.



session_id	pid	ppid	name	user	file
37	0	2400	svchost.exe	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
38	0	2428	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
39	0	2452	svchost.exe	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
40	0	2472	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
41	0	2488	svchost.exe	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
42	0	2504	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
43	0	2596	Memory Compression		
44	0	2648	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
45	0	2684	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
46	0	2852	igfxCUIService.exe	NT AUTHORITY\SYSTEM	C:\...
47	0	2892	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
48	0	2900	svchost.exe	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
49	0	3000	svchost.exe	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
50	0	2808	svchost.exe	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
51	0	2968	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
52	0	2840	svchost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
53	0	3104	wlanext.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\wlanext.exe
54	0	3116	conhost.exe	NT AUTHORITY\SYSTEM	C:\Windows\System32\conhost.exe

Şəkil 1 Tusp Paleon bazasının SQLiteStudio meneceri ilə görüntüsü

2.1 Tələblər

Paleon aşağıdakı əməliyyat sistemlərinin **32** və **64**-bit arxitektura malik versiyalarında sınaqlardan uğurla keçmişdir:

- Windows 7
- Windows 10
- Windows 11

Paleonun kritik sistem məlumatlarını əldə edə bilməsi üçün admin imtiyazlarına sahib istifadəçi tərəfindən işə salınması tələb olunur.

2.2 Hədəf sistemdə quraşdırılması və silinməsi

Paleon tək bir paket halında gəldiyi üçün heç bir quraşdırılmaya ehtiyac duymur. İstifadəçinin yalnız hədəf sistem-ə uyğun paketi endirib işə salması kifayətdir. Eyni şəkildə silinməsi üçün-də xüsusi heç bir əməliyyat tələb edilmir. Endirilən paketin hədəf sistemdən silinməsi kifayət edəcəkdir.

2.3 İşə salınma prosesi

İstifadəçi Paleon-u birbaşa icra edilə bilən fayl və ya Windows əmr lövhəsi (cmd.exe | powershell) üzərindən işə sala bilər. Hər hansı bir problem yaranmayacağı təqdirdə istifadəçi aşağıdakı ekran ilə qarşılaşacaq.

```
Tusi Paleon v1.0b - Malware Forensic Tool
Computer Emergency Response Center [AZ] - Malware Research Lab [mrl.cert.gov.az]

[Enter case description]:democase01

7-Zip (r) 23.00 (x86) : Igor Pavlov : Public domain : 2023-05-07

Scanning the drive:
2 folders, 2 files, 1676328 bytes (1638 KiB)

Creating archive: PL_REPORT.7z

Add new data to archive: 2 folders, 2 files, 1676328 bytes (1638 KiB)

Enter password (will not be echoed):

Files read from disk: 2
Archive size: 342591 bytes (335 KiB)
Everything is Ok
```

Şəkil 2 Paleon-un powershell terminalı üzərindən işə salınması

Şəkil 1-də istifadəçidən yerinə yetirilən əməliyyat üçün xüsusi qeydləri varsa onları daxil etməsi tələb edilir. Qeyd daxil edildikdən sonra Paleon sistem məlumatlarını toplamağa

başlayacaqdır. Toplanacaq məlumatlar və bu əməliyyat zamanı baş verə biləcək xəta mesajları Paleonun icra edildiyi cari qovluq içərisində **“report”** adlı alt qovluqda saxlanacaqdır.

- Toplanan məlumatlar: PLReport.db
- Xəta mesajları: PLog.log
- pf qovluğu: Windows Prefetch

Paleon toplanan sistem məlumatlarını saxlamaq üçün **SQLite3** məlumat bazası formatından istifadə edir. İstifadəçi istənilən SQLite meneceri ilə toplanan məlumatlara bax bilər və onların analizini həyata keçirə bilər. Son olaraq toplanan məlumatlar “PL_REPORT.7z” arxiv fayl içərisində (şifrələnmiş halda) toplanır. Arxiv faylının hazırlanmasında [7Zip](#) alətindən istifadə edilmişdir.

Sınaqlar zamanı toplama əməliyyatı 5 – 10 dəqiqə vaxt aralığında tamamlanmışdır.

3 Məlumat bazası strukturu və cədvəllər

Paleon tərəfindən toplanan sistem məlumatları PLReport.db faylı içərisində, aid olduqları qruplara uyğun şəkildə cədvəllərdə saxlanır. Aşağıda cədvəl adları göstərilmişdir.

Case	ARPTable	Autorun	Chrome	Disks
Process	TCPTable	Shares	Edge	System
Drivers	IPConfig	Hosts	Chrome	ImageFileExecutions
Services	UDPTable	ProfilesDir	Firefox	Evt_Defender1116
Tasks	DNSCache	Programs	IPRoute	Firewall
Modules	Handles	Prefetch	Run	Opera

3.1 Cədvəllər

3.1.1 “Case” cədvəli və strukturu

Case cədvəli içərisində ilkin başlanğıc zamanı hədəf haqqında məlumatlar saxlanılır. Cədvəl strukturu:

Sütun adı	Sütun açıklaması
-----------	------------------

description	Hədəf haqqında qeyd
engine_version	Paleon versiyası
machine_guid	Hədəf kompüterə aid unikal identifikator
curr_time	Cari vaxt

3.1.2 “Processes” cədvəli və strukturu

Paleon hədəf sistemdə işə salındığı an sistemdə fəaliyyət göstərən prosesləri və onlara aid məlumatları “Processes” cədvəli altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
session_id	Prosesin icra edildiyi sessiya identifikasiya nömrəsi
pid	Proses identifikatoru
ppid	Prosesi işə salan ana proses (parent) identifikatoru
name	Proses adı
user	Prosesin icra edildiyi host və istifadəçi adı
file	Proses tam fayl yolu
cmd	Proses komanda sətri
size	Proses fayl ölçüsü
protected_file	Faylın ƏS tərəfindən qorunub qorunmadığı haqqında məlumat
md5	Proses faylı md5 xəş summası
sha1	Proses fayl sha1 xəş summası
sha2	Proses fayl sha2 xəş summası
creation	Proses faylının yaradılma vaxt damğası
accessed	Proses faylının giriş vaxt damğası
modified	Proses faylının dəyişdirilmə vaxt damğası
attributes	Proses faylına aid atributlar
creation_time	Prosesin yaradılma vaxtı
wow64process	Prosesin 32-bit olub olmadığı

3.1.3 “Services” cədvəli və strukturu

Hədəf sistemdə fəaliyyət göstərən servislər və onlara aid məlumatlar “Services” cədvəli altında toplanır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
name	Servis adı
display	Servis ekran adı
type	Servis tipi
file	Servis tam fayl yolu
size	Servis faylının ölçüsü
protected_file	Faylın ƏS tərəfindən qorunub qorunmadığı haqqında məlumat
md5	Servis faylının md5 xəş summası
sha1	Servis faylının sha1 xəş summası
sha2	Servis faylının sha2 xəş summası
creation	Servis faylının yaradılma vaxt damğası
accessed	Servis faylının giriş vaxt damğası
modified	Servis faylının dəyişdirilmə vaxt damğası
attributes	Servis faylına aid atributlar

3.1.4 “Drivers” cədvəli və strukturu

Sistemdəki cihaz sürücüləri və bunlara aid məlumatlar bu cədvəl altında toplanır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
name	Sürücü adı
file	Sürücünün aid olduğu faylın tam yolu
size	Sürücü faylının ölçüsü
md5	Sürücü faylının md5 xəş summası
sha1	Sürücü faylının sha1 xəş summası
sha2	Sürücü faylının sha2 xəş summası
creation	Sürücü faylının yaradılma vaxt damğası
accessed	Sürücü faylının giriş vaxt damğası
modified	Sürücü faylının dəyişdirilmə vaxt damğası
attributes	Sürücü faylına aid atributlar

3.1.5 “Tasks” cədvəli və strukturu

Paleon sistemdə mövcud olan planlaşdırılmış tapşırıqlar siyahısı bu cədvəl altında toplayır. Cədvəl stukturu:

Sütun adı	Sütun açıqlaması
host	Tapşırığın aid olduğu host adı
name	Tapşırıq adı
author	Tapşırıq sahibi
task	İcra ediləcək tapşırıq
start_in	Tapşırığın icra ediləcəyi qovluq
runas	İşə salınacaq istifadəçi
triggers	Tetiklənmə səbəbi
last_run_time	Son işə düşmə vaxtı

3.1.6 “Users” cədvəli və strukturu

Paleon sistemdə aktiv olan istifadəçiləri və onlara aid məlumatları bu cədvəl altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
name	İstifadəçi adı
sid	İstifadəçi təhlükəsizlik identifikatoru
last_logon_time	İstifadəçinin sistemə son giriş tarixi

3.1.7 “Windows” cədvəli və strukturu

Sistem aktiv pəncərələr və onlara aid məlumatlar bu cədvəl altında saxlanır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
pid	Pəncərənin aid olduğu proses identifikatoru
title	Pəncərə başlığı

3.1.8 “Disks” cədvəli və strukturu

Sistemdəki sərt disklər və onlara aid məlumatlar “Disks” cədvəlində toplanır. Cədvəl strukturu:

Sütun adı	Sütun açıklaması
label	Disk etiketi
name	Disk adı
serialnumber	Disk seriya nömrəsi
filesystem	Disk fayl sistemi
device	Disk sürücü adı
freebytesavailabletocaller	Çağıran üçün boş baytlar
totalnumberofbytes	Bayt cinsindən ümumi həcm
totalnumberoffreebytes	Bayt cinsindən ümumi boş həcm

3.1.9 “Autorun” cədvəli və strukturu

Sistemdə növbəti işə salınma zamanı avtomatik işə düşəcək proqramların siyahısı (bütün istifadəçilər üçün) bu cədvəl altında toplanır. Cədvəl strukturu:

Sütun adı	Sütun açıklaması
key	Avtomatik işə düşəcək proqramın Windows reyest açarı
name	Proqram reyestr adı
data	Proqram yolunun olduğu reyestr dəyəri

3.10.1 “Evt_Defender1116” cədvəli və strukturu

Windows 10 əməliyyat sistemi ilə defolt olaraq gələn zərərvericilərə qarşı qoruma proqramı “Windows Defender” real vaxt rejimində hər hansı bir zərərverici aşkarladığı zaman bunu raportlamaq üçün 1116 identifikasiya nömrəli xüsusi hadisə (event) yaradır. Paleon hadisələr içərisindən 1116 identifikasiya nömrəsinə malik hadisələri təhlil edir və bunları “Evt_Defender1116” cədvəlində toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıklaması
detection_time	Zərərvericinin aşkarlanma vaxtı
threat_name	Defender tərəfindən zərərvericiyə təyin edilən ad
process_name	Zərərvericini tetikləyən proses
detection_user	Zərərvericinin aşkarlandığı istifadəçi
path	Zərərverici faylın yolu

3.1.11 “ImageFileExecutions” cədvəli və strukturu

Windows əməliyyat sistemində IFEO zərərvericilər tərəfindən hər hansı bir proqramı başqa bir proqrama yönləndirmək üçün istifadə olunan bir mexanizmdir. Normal şəraitdə bu mexanizm hər hansı proqramın icra edilməsi zamanı xəta baş verər isə avtomatik şəkildə debugger alətini işə salmaq üçün nəzərdə tutulub. Lakin zərərvericilər bu mexanizmi debug aləti əvəzinə proqramı zərərverici proqrama yönləndirmək üçün istifadə edirlər. Paleon yönləndirilən proqramların siyahısını bu cədvəl altında toplayır (bütün istifadəçilər üçün). Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
name	Yönləndirilmək istənen proses adı
value	Yönləndirilən proqram

3.1.12 “Programs” cədvəli və strukturu

Paleon bu cədvəl altında sistemə quraşdırılan proqram təminatlarına aid məlumatları toplayır (bütün istifadəçilər üçün). Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
name	Quraşdırılan proqramın adı
version	Quraşdırılan proqramın versiyası
install_date	Quraşdırılma vaxtı

3.1.13 “IPConfig” cədvəli və strukturu

Sistemə aid əldə edilən IP konfigurasiya [ipconfig /all] məlumatları bu cədvəl altında toplanır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
content	ipconfig /all

3.1.14 “DNSCache” cədvəli və strukturu

Ziyarət edilən DNS adreslərin resolver keş məlumatları bu cədvəl altında toplanır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
-----------	------------------

content	ipconfig /displaydns
---------	----------------------

3.1.15 “Hosts” cədvəli və strukturu

Bu cədvəl altında hosts faylının kontenti saxlanılır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
content	Hosts faylının tərkibi

3.1.16 “Firewall” cədvəli və strukturu

Paleon “Windows Firewall” qaydalarını bu cədvəl altında saxlayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
name	Qayda adı
rule	Qayda

3.1.17 “Shares” cədvəli və strukturu

Sistem paylaşımaları və onlara aid məlumatlar bu cədvəl altında toplanır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
name	Paylaşım adı
path	Paylaşılan qovluq
install_current_uses	Cari paylaşımından istifadələrin sayı

3.1.18 “IPRoute” cədvəli və struktur

Paleon şəbəkə IPv4 marşrutlaşdırma cədvəlini və ona aid məlumatları bu cədvəl altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
destination	Təyinat ünvanı
subnet	Alt şəbəkə maskası
gateway	Qapı (marşrutda növbəti sistem)
adapter	Bağlı olduğu adapter index nömrəsi

type	Marşrut tipi
protocol	Protokol

3.1.19 “TCPTable” cədvəli və strukturu

Paleon hədəf sistem IPv4 TCP bağlantılarını və onlara aid məlumatları bu cədvəl altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
pid	Bağlantı yaradan prosesin identifikatoru
local_addr	Bağlantı lokal adresi
local_port	Bağlantı local portu
remote_addr	Bağlantı qurulan adres
remote_port	Bağlantı qurulan port

3.1.20 “UDPTable” cədvəli və strukturu

Paleon hədəf sistem IPv4 UDP məlumatları bu cədvəl altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
pid	Bağlantı yaradan prosesin identifikatoru
local_addr	Bağlantı lokal adresi
local_port	Bağlantı local portu

3.1.21 “ARPTable” cədvəli və strukturu

Paleon hədəf sistem IPv4 ARP (Address Resolution Protocol) xəritələndirmə məlumatlarını bu cədvəl altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
inet_addr	İnternet adresi
physical_addr	Fiziki ünvan

3.1.22 “System” cədvəli və strukturu

Paleon hədəf sistem haqqında ekspertiza zamanı lazım ola biləcək məlumatları bu cədvəl altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıklaması
system	Sistem (Windows)
version	Sistem versiyası;
os	Əməliyyat sistemi geniş məlumat
processor	Prossesor haqqında məlumat
release	Reliz versiyası
current_user	Paleonun işə salan istifadəçi
host	Host(kompüter) adı
windir	Windows qovluq yolu
sysdir	System32 qovluq yolu
profiles_dir	İstifadəçilərə aid profil qovluq yolu
locale	
current_time	Paleon işə salınan zaman sistem vaxtı

3.1.23 “Firefox tablosu” və strukturu

Paleon hədəf sistemdə mövcud olar isə “Mozilla Firefox” web bələdçisi ilə ziyarət edilən URL ünvanların siyahısını (bütün istifadəçilər və profillər üçün) bu cədvəl altında toplayır. **Not:** Bələdçi aktiv olmamalıdır . Cədvəl strukturu:

Sütun adı	Sütun açıklaması
title	Sayt başlığı
url	Url ünvan
last_visit_time	Son ziyarət vaxt damğası

3.1.24 “Chrome” cədvəli və strukturu

Paleon hədəf sistemdə mövcud olar isə “Google Chrome” web bələdçisi ilə ziyarət edilən URL ünvanların siyahısını (bütün istifadəçilər və profillər üçün) bu cədvəl altında toplayır. **Not:** Bələdçi aktiv olmamalıdır. Cədvəl strukturu:

Sütun adı	Sütun açıklaması
title	Sayt başlığı
url	Url ünvan
last_visit_time	Son ziyarət vaxt damğası

3.1.25 “Edge” cədvəli və strukturu

Paleon hədəf sistemdə mövcud olar isə “Microsoft Edge” web bələdçisi ilə ziyarət edilən URL ünvanların siyahısını (bütün istifadəçilər və profillər üçün) bu cədvəl altında toplayır. **Not:** Bələdçi aktiv olmamalıdır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
title	Sayt başlığı
url	Url ünvan
last_visit_time	Son ziyarət vaxt damğası

3.1.26 “Opera” cədvəli və strukturu

Paleon hədəf sistemdə mövcud olar isə “Opera” web bələdçisi ilə ziyarət edilən URL ünvanların siyahısını (bütün istifadəçilər və profillər üçün) bu cədvəl altında toplayır. **Not:** Bələdçi aktiv olmamalıdır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
title	Sayt başlığı
url	Url ünvan
last_visit_time	Son ziyarət vaxt damğası

3.1.27 “Run” cədvəli və strukturu

Paleon hədəf sistemdə run əmr tarixini bu cədvəl altında toplayır. Cədvəl strukturu:

Sütun adı	Sütun açıqlaması
key	Əmrin reyest açarı
command	Əmr

3.1.28 “Prefetch” cədvəli və strukturu

Paleon hədəf sistemdə mövcud olan prefetch fayllarını cari işə düşdüyü qovluğun pf adlı alt qovluğunda toplayır. Toplanan fayllar Prefetch cədvəlinə yazılır.

Sütun adı	Sütun açıqlaması
filename	“pf” qovluğuna kopyalanan prefetch fayl adı

3.1.29 “Evt_UsrLogon_4624”

Paleon hədəf sistemdə istifadəçi girişləri haqqında məlumat bu cədvəl altında toplayır.

Sütun adı	Sütun açıqlaması
subject_username	Giriş haqqında məlumat verən istifadəçi
target_username	Girişi həyata keçirən istifadəçi
process_name	Əməliyyat icra edən proses
ip_address	Uzaq girişlər zamanı giriş edən komputer ip adresi
logon_type	Giriş tipi