

Forenzika log datoteke

Kristian Skračić

Petar Djeramimović

Predrag Pale





Zašto forenzika log datoteka?

- **problemi** u sustavu
- obično postaju **očiti**
- tek **nakon** događaja koji ih je uzrokovao
 - ponekad **puno kasnije**:
 - dani, tjedni, mjeseci
- Čak i ako pratimo događaje dok se događaju
 - moguće je da čemo trebati znati kada se sličan događaj desio u **prošlosti**
- stoga, imamo potrebu **istraživati prošle** događaje
- Srećom **postoji način** da se to postigne
- postoje **zаписи дешављаја** (eng. **event logs**) na sustavu
 - stvara ih operacijski sustav, servisi i aplikacije
 - često
 - arhiviraju se mjesečno, godišnje





linux logovi



Linux logovi



- Obično **pohranjeni** u tekstualnom (ASCII) obliku
 - **Jedan redak** predstavlja **jedan događaj**
 - Ponekad je problematično naći
u kojem se logu nalaze informacije
koje su nam potrebne
-
- No, sama analiza je jednostavna
 - jer se najčešće radi o čitljivom/tekstualnom formatu
 - Nažalost – ovo svojstvo koriste i zlonamjernici
 - za pronalaženje vlastitih tragova
 - i njihovo brisanje





User activity logs

- Prijave i odjave korisnika
 - [/var/run/utmp](#)
 - Sadrži informacije samo za aktivne prijave
 - [/var/log/wtmp](#)
 - Za dulje čuvanje informacija o prijavama
- [/var/log/lastlog](#)
 - binarni log
 - Sadrži informacije o zadnjoj prijavi svih korisnika
 - » Vrijeme prijave,
 - » remote host



/var/log/wtmp



user:~\$ last -f wtmp.1

Korisnik		dolazi s računala
its	pts/0	dhcp-154.zesoi.f Thu Dec 31 17:45 - 18:22 (00:37)
ppale	pts/1	dhcp-93.zesoi.fe Sat Dec 26 11:30 - 18:37 (07:06)
ppale	pts/1	dhcp-93.zesoi.fe Sat Dec 26 11:26 - 11:30 (00:04)
ppale	pts/1	dhcp-93.zesoi.fe Sat Dec 26 11:19 - 11:26 (00:06)
its	pts/0	dhcp-154.zesoi.f Sat Dec 26 11:00 - 09:48 (1+22:48)
its	pts/0	dhcp-154.zesoi.f Fri Dec 25 22:13 - 22:48 (00:35)
its	pts/0	dhcp-154.zesoi.f Wed Dec 23 10:18 - 10:38 (00:20)
reboot	system boot	3.16.0-4-amd64 Wed Dec 23 10:18 - 23:49 (21+13:30)
its	pts/0	dhcp-154.zesoi.f Wed Dec 23 10:16 - 10:18 (00:02)
its	pts/0	dhcp-154.zesoi.f Fri Dec 11 09:14 - 09:38 (00:24)
reboot	system boot	3.16.0-4-amd64 Fri Dec 11 09:13 - 10:18 (12+01:04)
its	pts/0	dhcp-154.zesoi.f Fri Dec 11 09:12 - 09:13 (00:01)
its	pts/0	dhcp-154.zesoi.f Thu Dec 10 15:52 - 16:33 (00:41)
reboot	system boot	3.16.0-4-amd64 Fri Dec 4 15:40 - 09:13 (6+17:33)
its	pts/0	dhcp-154.zesoi.f Fri Dec 4 15:10 - 15:12 (00:02)



/var/log/lastlog



```
ppale@maja:/var/log$ lastlog
```

Username	Port	From	Latest
root	tty1		Fri Jul 31 07:09:26 +0200 2015
mail			**Never logged in**
news			**Never logged in**
postfix			**Never logged in**
postgrey			**Never logged in**
amavis			**Never logged in**
ppale	pts/0	dhcp-73.zesoi.fe	Wed Jan 13 23:47:48 +0100 2016
its	pts/0	dhcp-154.zesoi.f	Wed Jan 13 11:09:51 +0100 2016
proftpd			**Never logged in**
ftp			**Never logged in**
nagios			**Never logged in**
nastava			**Never logged in**
messagebus			**Never logged in**
dovecot			**Never logged in**
jpetrovic	pts/0	2001:b68:16:70:1	Thu Nov 19 13:06:57 +0100 2015
clamav			**Never logged in**
vkezdorf	pts/0	dhcp-94.zesoi.fe	Fri Jul 12 09:07:50 +0200 2013
debian-spamd			**Never logged in**
ntp			**Never logged in**



Syslog



- Većina Linux logova pohranjeni su u
 - `/var/log`
 - bilo u vršnom direktoriju
 - bilo u poddirektorijima
 - Syslog koristi client/server model
 - što omogućuje pohranu logova na udaljenom računalu
- Syslog koristi
 - „*facility/priority*” sustav klasifikacije praćenih događaja
 - “*facility*” = tko (koji program) je prijavio događaj
 - “*priority*” = koliko je važan taj događaj

<code>/var/log/messages</code>
<code>/var/log/auth.log</code>
<code>/var/log/sulog</code>
<code>/var/log/httpd/*</code>
<code>/var/log/samba/smbd.log</code>
<code>/var/log/audit/audit.log</code>
<code>/var/log/maillog</code>
<code>/var/log/cron</code>
<code>/var/log/xferlog</code>



Syslog facility



Auth	Authentication activity
Authpriv	Authentication and PAM messages
Cron	Cron/At/Task Scheduler messages
Daemon	Daemons/service messages
Kern	Kernel messages
Lpr	Printing services
Mail	Email (imap, pop, smtp) messages
News	Usenet News Server messages
Syslog	Messages from syslog
User	User program messages
Local	Locally defined



Syslog priority

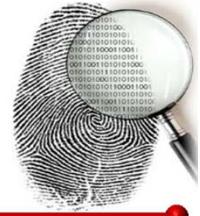


Syslog ljestvica važnosti događaja

Emerg or Panic	System is unusable
Alert	Action must be taken immediately
Crit	Critical conditions
Err	Error conditions
Warning	Warning conditions
Notice	Normal but significant conditions
Info	Informational messages
Debug	Debugging level messages, very noisy
None	Used to override (*) wildcard
*	All levels except none



Syslog sadržaj



- **Vrijeme i datum** stvaranja poruke/događaja
- **Naziv računala** (host name)
na kojemu se poruka/događaj dogodila
- Naziv **procesa** koji je napravio poruku/događaj
- **Tekst** poruke/događaja



Syslog primjer



Time stamp	Host	Process	Message
Mar 7 04:02:08	avas	syslogd	1.4.1: restart.
Mar 7 04:02:16	avas	clamd[11165]	: /var/amavis/amavis-20040307T033734-10329/parts/part-00003: Worm.Mydoom.F FOUND
Mar 7 04:05:55	avas	clamd[11240]	: /var/amavis/amavis-20040307T035901-10615/parts/part-00002: Worm.SomeFool.Gen-1 FOUND
Mar 7 04:11:15	avas	dccifd[11335]	: write(MTA socket,4): Broken pipe
Mar 7 04:14:12	avas	clamd[11346]	: /var/amavis/amavis-20040307T033734-10329/parts/part-00002: Worm.SomeFool.Gen-2 FOUND
Mar 7 04:58:25	avas	clamd[27173]	: SelfCheck: Database status OK.
Mar 7 05:20:01	avas	clamd[20434]	: /var/amavis/amavis-20040307T051352-20223/parts/part-00003: Worm.Mydoom.F FOUND
Mar 7 05:59:01	avas	clamd[27173]	: SelfCheck: Database modification detected. Forcing reload.
Mar 7 05:59:01	avas	clamd[27173]	: Reading databases from /usr/local/share/clamav
Mar 7 05:59:02	avas	clamd[27173]	: Database correctly reloaded (20400 viruses)
Mar 7 06:12:56	avas	dccifd[21165]	: write(MTA socket,4): Broken pipe



Useful log files



/var/log/messages	Catch-all, nonspecified logs
/var/log/auth.log	User authentication successes/failures
/var/log/sulog	“su” attempts/success
/var/log/httpd/*	Apache Web Server
/var/log/samba/smbd.log	Samba (Windows File Sharing)
/var/log/audit/audit.log	Auditd/SELinux
/var/log/maillog	Mail servers (sendmail/postfix)
/var/log/cron	Anacron/cron
/var/log/xferlog	FTP servers



Syslog karakteristike



- Uniforman format čini ih jednostavnim za pretraživanje
- Većina Linux sustava koristi neki oblik „rotacije“ logova
 - npr. svaki mjesec se svi postojeći logovi komprimiraju u Gzip arhivu, te se otvaraju novi za taj mjesec
 - serveri će vjerojatno puno češće napraviti rotaciju zbog veće količine logova





Drugi zanimljivi artefakti na Linuxu

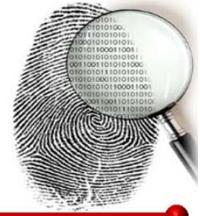




- Sve datoteke potrebne za korištenje SSH
 - se nalaze u korisničkom (home direktoriju)
- **.ssh/known_hosts**
 - kada se korisnik prijavi putem SSH,
u ovu datoteku se pohranjuje
 - IP adresa računala udaljenog korisnika
 - Naziv računala (host name)
 - Javni ključ
 - Neke Linux distribucije
 - omogućuju hash-iranje ove datoteke



.ssh/known_hosts

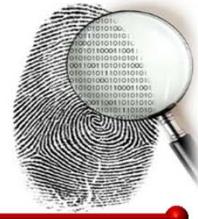


```
$ cat .ssh/known_hosts
```

```
192.168.0.106 ssh-
rsaAAAAB3NzaC1yc2EAAAQABAAQDRtd74Cp19PO44
zRDUDmK0EmkuD/d4WAefzPaf55L5Dh5C06Sq+xG543sw0i1LjMN7C
IJbz+AnSd967ax/BZZimUchHk8gm2BzoAEbp0EPIJ+G2vLOrc+faM
1NZhDDzGuoFV7tMnQQLOrqD9/4PfC1yLGV1IJ9obd+6BR78yeBRdq
HVjYsKUTJl46aKoVwV60dafV1Efbojh1/zKhhliKAaY1LhXALnp8/
18EBj5CDqsTKCcGQbhkSPgYgxuDg8qD7ngLpB9oUvV9QSDZkmR0R937MY
i
IpUYPqdK5opLVnKn81B1r+TsTxii7RJ7M53p0cvx8nNf jwAuNzWTLJz6z
r
```



.ssh/known_hosts – uz hashiranje



| 1 | rjAWXFqldZmjmgJnaw7HJ04KtAg= | qfrtMVerwngkTaW
C7mdEF3HNx/o=

ssh-

rsaAAAAB3NzaC1yc2EAAAQABAAQDRtd74Cp19P044
zRDUDMk0EmkuD/d4WAefzPaf55L5Dh5C06Sq+xG543sw0i1
LjMN7CIJbz+AnSd967aX/BZZimUchHk8gm2BzoAEbp0EPIJ
+G2vLOrc+faM1NZhDDzGuoFV7tMnQQLOrqD9/4PfC1yLGv1
IJ9obd+6BR78yeBRdqHVjYsKUTJ146aKoVwV60dafV1Efbo
jh1/ZKhhliKAaY1LhXALnp8/18EBj5CDqsTKCcGQbhkSPgY
gxuDg8qD7ngLpB9oUvV9QSDZkmR0R937MYiIpUYPqdK5opL
VnKn81B1r+TsTxidI7RJ7M53p0cvx8nNf jwAuNzWTLJz6zr



Logs of command line interface



- Bash je najčešće (default) korisničko sučelje (ljudska) za većinu Linux sustava
- `~/.bash_history`
 - sadrži “povijest” Bash ljudske
 - tj, prethodno izdane naredbe
 - svaki korisnik ima vlastitu povijest
 - obično nemaju vremenske oznake 😞
 - već samo niz naredbi koje su zadane i izvršene

```
ls -al
rm comfor_automat
mkdir comfor_automat
ls -al
chmod -R g+w comfor_automat/
cd comfor_automat/
nano program
ls -al
chmod +x program
./program
nano program
./program
nano /etc/postfix/aliases
exit
l pr*
```





- Velik broj zločudnih aplikacija
- često mijenja korisnikov DNS sustav
 - kako bi legitiman promet preusmjerila na vlastite poslužitelje
 - Man-in-the-middle ili
 - Phishing napad
 - /etc/resolv.conf
 - mnogi Linux sustavi ga koriste za konfiguraciju DNS-a
 - /etc/hosts
 - Služi za mapiranje IP adresa na DNS adrese

```
/etc > more resolv.conf
nameserver 161.53.64.4
nameserver 161.53.64.60
nameserver 161.53.64.61
```

```
maja:~$ more /etc/hosts
127.0.0.1      localhost
161.53.64.3    maja.zesoi.fer.hrmaja

# The following lines are desirable
# for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

2015-12-30
```





Forenzika Windows logova





- Windows logovi (pre-Vista):
 - Windows 2000, XP, Server 2003
 - Binarne datoteke, ekstendija: .evt
 - Najvažniji logovi:
 - System
 - Security
 - Application
 - c:\windows\system32*.evt
- Windows logovi (Vista i novije):
 - Vista, 7, 8, 10
 - Binarne datoteke/XML format, .evtx
 - Najvažniji logovi:
 - System
 - Security
 - Application
 - Mnogo novih logova (specifičnih za određene aplikacije)
 - c:\windows\system32\winevt\Logs*.evt x

Predavanje će biti usmjereni na novi format logova



Koliko novih logova?



Logs

File Home Share View

Computer > Local Disk (C:) > Windows > System32 > winevt > Logs

The screenshot shows a Windows File Explorer window displaying a list of log files located at C:\Windows\System32\winevt\Logs. The files are organized into three columns. The first column contains logs from the Application, Security, and System event providers, which are circled in red. The second and third columns contain numerous Microsoft Windows system logs. At the bottom of the window, it shows there are 250 items, 1 item selected (Security.evt), and the total size is 20.0 MB.

Log Type	File Name
Event Providers	Application.evtx
	Security.evtx
	System.evtx
Microsoft-Windows-GroupPolicy%4Operational.evtx	
Microsoft-Windows-PowerShell%4Operational.evtx	
Microsoft-Windows-User Profile Service%4Operational.evtx	
Windows PowerShell.evtx	
ACEEventLog.evtx	
Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	
Microsoft-Windows-Application-Experience%4Program-Inventory.evtx	
Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx	
Microsoft-Windows-AppModel-Runtime%4Admin.evtx	
Microsoft-Windows-AppXDeployment%4Operational.evtx	
Microsoft-Windows-AppXDeploymentServer%4Operational.evtx	
Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx	
Microsoft-Windows-AppxPackaging%4Operational.evtx	
Microsoft-Windows-Audio%4PlaybackManager.evtx	
Microsoft-Windows-BackgroundTaskInfrastructure%4Operational.evtx	
Microsoft-Windows-Bits-Client%4Operational.evtx	
Microsoft-Windows-CertificateServicesClient-Lifecycle-User%4Operational.evtx	
Microsoft-Windows-CodeIntegrity%4Operational.evtx	
Microsoft-Windows-DeviceSetupManager%4Admin.evtx	
Microsoft-Windows-DeviceSetupManager%4Operational.evtx	
Microsoft-Windows-Dhcp-Client%4Admin.evtx	
Microsoft-Windows-Dhcpv6-Client%4Admin.evtx	
Microsoft-Windows-Diagnosis-DPS%4Operational.evtx	
Microsoft-Windows-Diagnosis-PCW%4Operational.evtx	
Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx	
Microsoft-Windows-Diagnosis-Scripted%4Admin.evtx	
Microsoft-Windows-Diagnosis-Scripted%4Operational.evtx	
Microsoft-Windows-Diagnostics-Performance%4Operational.evtx	
Microsoft-Windows-Fault-Tolerant-Heap%4Operational.evtx	
Microsoft-Windows-Hyper-V-VMMS-Admin.evtx	
Microsoft-Windows-Kernel-PnP%4Configuration.evtx	
Microsoft-Windows-Kernel-PnPConfig%4Configuration.evtx	
Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx	
Microsoft-Windows-Kernel-WHEA%4Operational.evtx	
Microsoft-Windows-Known Folders API Service.evtx	
Microsoft-Windows-LanguagePackSetup%4Operational.evtx	
Microsoft-Windows-LiveId%4Operational.evtx	
Microsoft-Windows-NetworkProfile%4Operational.evtx	
Microsoft-Windows-PrintService%4Admin.evtx	
Microsoft-Windows-PushNotification-Platform%4Operational.evtx	
Microsoft-Windows-ReadyBoost%4Operational.evtx	
Microsoft-Windows-ReliabilityAnalysisComponent%4Operational.evtx	
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx	
Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx	
Microsoft-Windows-SettingSync%4Debug.evtx	
Microsoft-Windows-SettingSync%4Operational.evtx	
Microsoft-Windows-Shell-Core%4Operational.evtx	
Microsoft-Windows-SMBClient%4Operational.evtx	
Microsoft-Windows-TaskScheduler%4Maintenance.evtx	
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	
Microsoft-Windows-TerminalServices-RDPCClient%4Operational.evtx	
Microsoft-Windows-TerminalServices-Remot	
Microsoft-Windows-TerminalServices-Remot	
Microsoft-Windows-TWinUI%4Operational.e	
Microsoft-Windows-UAC-FileVirtualization%4	
Microsoft-Windows-Wcmsvc%4Operational.e	
Microsoft-Windows-WER-Diag%4Operational	
Microsoft-Windows-Windows Defender%4Op	
Microsoft-Windows-Windows Defender%4Wf	
Microsoft-Windows-Windows Firewall With A	
Microsoft-Windows-WindowsSystemAssessm	
Microsoft-Windows-WindowsUpdateClient%	
Microsoft-Windows-WMI-Activity%4Operatio	
Microsoft-WS-Licensing%4Admin.evtx	
OAlerts.evtx	
Operational.evtx	
Setup.evtx	
ConnectionInfo.evtx	
Error.evtx	
HardwareEvents.evtx	
Internet Explorer.evtx	
Key Management Service.evtx	
Microsoft-Rdms-UI%4Admin.evtx	
Microsoft-Rdms-UI%4Operational.evtx	
Microsoft-Windows-All-User-Install-Agent%4	
Microsoft-Windows-Anytime-Upgrade-Event:	
Microsoft-Windows-AppHost%4Admin.evtx	
Microsoft-Windows-AppID%4Operational.evt	

Poznatiji pregled logova



- Koristeći „MMC console event viewer snap-in”, slično Event Viewer alatu u prijašnjim inačicama

Screenshot of the MMC Console window showing the Event Viewer snap-in.

The title bar reads "Console1 - [Console Root\Event Viewer (Local)\Windows Logs\System]".

The left pane shows the navigation tree:

- Console Root
 - Event Viewer (Local)
 - Custom Views
 - Windows Logs
 - Application
 - Security
 - Setup
 - System**
 - Forwarded Events
 - Applications and Services Logs
 - Subscriptions

The main pane displays a table of events from the System log:

Level	Date and Time	Source
Warning	19-Jan-16 11:10:52	Display
Warning	19-Jan-16 7:38:23	DNS Client Events
Error	18-Jan-16 13:13:42	DistributedCOM
Information	18-Jan-16 12:00:00	EventLog
Error	18-Jan-16 11:20:45	DistributedCOM
Error	18-Jan-16 8:00:16	Schannel
Error	18-Jan-16 8:00:16	Schannel
Information	18-Jan-16 3:26:46	Kernel-General
Information	18-Jan-16 3:26:46	Kernel-General
Information	18-Jan-16 3:26:46	Kernel-General
Information	18-Jan-16 3:26:45	Kernel-General
Information	18-Jan-16 3:26:33	Kernel-General
Error	17-Jan-16 21:14:56	Schannel
Error	17-Jan-16 21:14:56	Schannel
Error	17-Jan-16 14:46:16	Schannel
Error	17-Jan-16 14:46:16	Schannel
Information	17-Jan-16 12:00:00	EventLog
Information	17-Jan-16 3:22:47	Kernel-General
Information	17-Jan-16 3:22:47	Kernel-General
Information	17-Jan-16 3:22:46	Kernel-General
Information	17-Jan-16 3:22:44	Kernel-General

The right pane shows the "Actions" menu for the selected event (Event 4101, Display):

- System
 - Open Saved Log...
 - Create Custom View...
 - Import Custom View...
 - Clear Log...
 - Filter Current Log...
 - Properties
 - Find...
 - Save All Events As...
 - Attach a Task To this Log...
- View
 - New Window from Here
- Refresh
- Help

The bottom pane shows the details of the selected event (Event 4101, Display):

General tab content:
Display driver amdkmdap stopped responding and has successfully recovered.

Details tab content:
Log Name: System
Source: Display
Legend: 10-Jan-16 11:10:52

Page footer: Computer forensics - Logs 2015-12-30



Format poruka

- Svaka poruka sastoji se od dva dijela:
 - Struktura poruke
 - Definirana u biblioteci koja sadrži zapis za sve poruke iste vrste
 - Podatci poruke
 - Pohranjeni u .evtx datotekama
- Struktura poruke se ponekad definira u zasebnoj datoteci
 - Koju dostavlja treća strana
(npr. stvaratelj poruke nekog loga)
- Uobičajeno se prilikom instalacije aplikacije dodaju 3 nove datoteke koje sadrže poruke s metapodatcima koje se registriraju
 - i registarski ključ se stvara (CategoryMessageFile, EventMessageFile, ParameterMessageFile)
- Svi ključevi (za različite aplikacije koje proizvode poruke) su u
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog*



Primjer: display driver warning



($4101_{(10)}=1005_{(16)}$; $28582_{(10)}=6FA6_{(16)}$; entries are LE)

The screenshot displays two windows side-by-side: Event Viewer and Registry Editor.

Event Viewer (Left):

- Shows two warning events from the **Display** provider.
- The first event has **Event ID 4101**.
- The second event has **Event ID 1014 (1014)**.
- The XML view of the first event includes the following details:
 - Provider Name = **Display**
 - EventID Qualifiers = **0x4101**
 - Level = **3**
 - Task = **0**
 - Keywords = **0x8000000000000000**
 - TimeCreated SystemTime = **2016-01-19T10:10:52**
 - EventRecordID = **28582**
 - Channel = **System**
 - Computer = **sobica**
 - Security = **<Security />**
 - Data = **amdkmdap**

Registry Editor (Right):

- Shows the registry key **Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\amdkmdap**.
- Subkeys include: 3ware, ACPI, adp94xx, adpahci, adpu320, AeLookupSvc, AllUserInstallAgent, AmdK8, amdkmdag, **amdkmdap**, AmdPPM, and amdsata.
- The data pane shows the binary representation of the registry entries. Several bytes are circled in red or blue:

 - Red circles highlight the bytes **A6 6F 00 00 00 00** at offset **00E4C5D0** and the string **a.m.d.k.m.d.a.p** starting at offset **00E4C610**.
 - Blue circles highlight the bytes **05 10** at offset **00E4C5B0** and the string **.a.m.d.k.m.d.a.p** starting at offset **00E4C610**.



Događaji vezani uz sigurnost



- Revizijski kodovi, mogu biti **uspješne** ili **neuspješne**
- Kratko objašnjenje dostupno u “properties”->”Explain” opciji u *Group Policy Editor* alatu
- Identifikatori (ID) ovise o inačici Windows sustava
 - Alternativno, većina revizijskih kodova je dostupna na webu (<https://support.microsoft.com/en-us/kb/977519>)
- Alternativno, moguće je od Microsoft-a preuzeti
 - **xls tablice i tekstualne datoteke s popisom događaja i kodova**
- Događaji koji se bilježe ovise o konfiguraciji
 - **Revizijska politika (eng. audit policy)**
- Zanimljivi događaji su obično prijave i odjave korisnika, neuspješne prijave, eskalacija ovlasti na sustavu i slično



Konfiguracija sigurnosnih događaja



Console1 - [Console Root\Local Computer Policy\Computer Configuration\Windows Settings\Security Options]

File Action View Favorites Window Help

Back Forward Refresh Stop Help Contents

Console Root

Local Computer Policy

- Computer Configuration
 - Software Settings
 - Windows Settings
 - Name Resolution Policies
 - Scripts (Startup/Shutdown)
 - Deployed Printers
 - Security Settings
 - Account Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options
 - Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options
 - Windows Firewall with Advanced Security
 - Network List Manager
 - Public Key Policies
 - Software Restrictions
 - Application Control Policies
 - IP Security Policies
 - Advanced Audit Policies
 - Policy-based QoS
 - Administrative Templates

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Actions
Audit Policy
More Actions

- Konfiguracija se može mijenjati putem alata gpedit.msc ili MMC (Group Policy Object Editor)
- Zadane vrijednosti ovise o inačici Windows sustava
 - npr. samo uspješne prijave na desktop računalima, i uspješne i neuspješne prijave na serverima



Sistemski događaji



- Zapisi koje stvara:
 - Operacijski sustav, i njegovi servisi
- Najzanimljiviji događaji su
 - Pokretanje i zaustavljanje servisa
 - Pokretanje i zaustavljanje operacijskog sustava
 - Promjene sistemskog vremena
- Zaustavljanje računala se ponekad ne bilježi
 - Zbog neočekivanog zaustavljanja (npr. ispad sustava)
- Korisno za korelaciju s drugim tragovima
 - Promjene vremena su posebno značajne
- Razine:
 - error, warning, information



Aplikacijski događaji



- Također tri razine (Error, Warning, Information)
- MSDN smjernice
 - Error: nije moguće nastaviti s dalnjim radom aplikacije
 - Npr. Ispad zbog nedostatka memorije
 - Warning: ne-kritičan događaj koji bi u budućnosti mogao izazvati ispad
 - Npr. Uspješno pisanje na korumpirani sektor nakon drugog pokušaja
 - Information: uspješno obavljena operacija
 - Npr. Uspješna prijava na bazu
- Aplikacija odlučuje hoće li koristiti Windows događaje
 - te kako će klasificirati svoje događaje prema postojećim smjernicama
- Korisno kada se istražuje određena aplikacija





Za sve logove

- „Glasni“
 - = sadrže obilje informacije
- Ovise o konfiguraciji
- Više potencijalnih točaka za neovlašteni pristup
 - Izmjena biblioteka (DLL) drugih proizvođača
- Obično ne predstavljaju primarne dokaze
 - Ali korisno za korelaciju s drugim dokazima



Windows Registry





Windows registry je ...

- jedna od osnovnih komponenti svakog operacijskog sustava Windows
- dio sustava od verzije Windows 3.1 (1992!)
- hijerarhijska baza podataka
 - kojom upravlja operacijski sustav
 - a služi za pohranu konfiguracijskih podataka
 - komponenti sustava i korisničkih aplikacija
- zamjena za “ini datoteke”
 - iz ranijih verzija Microsoftovih sustava (DOS)
- zanimljiv izvor tragova
 - u forenzičkoj analizi strojeva s Windows OS-om





Programski pristup živom registry-u

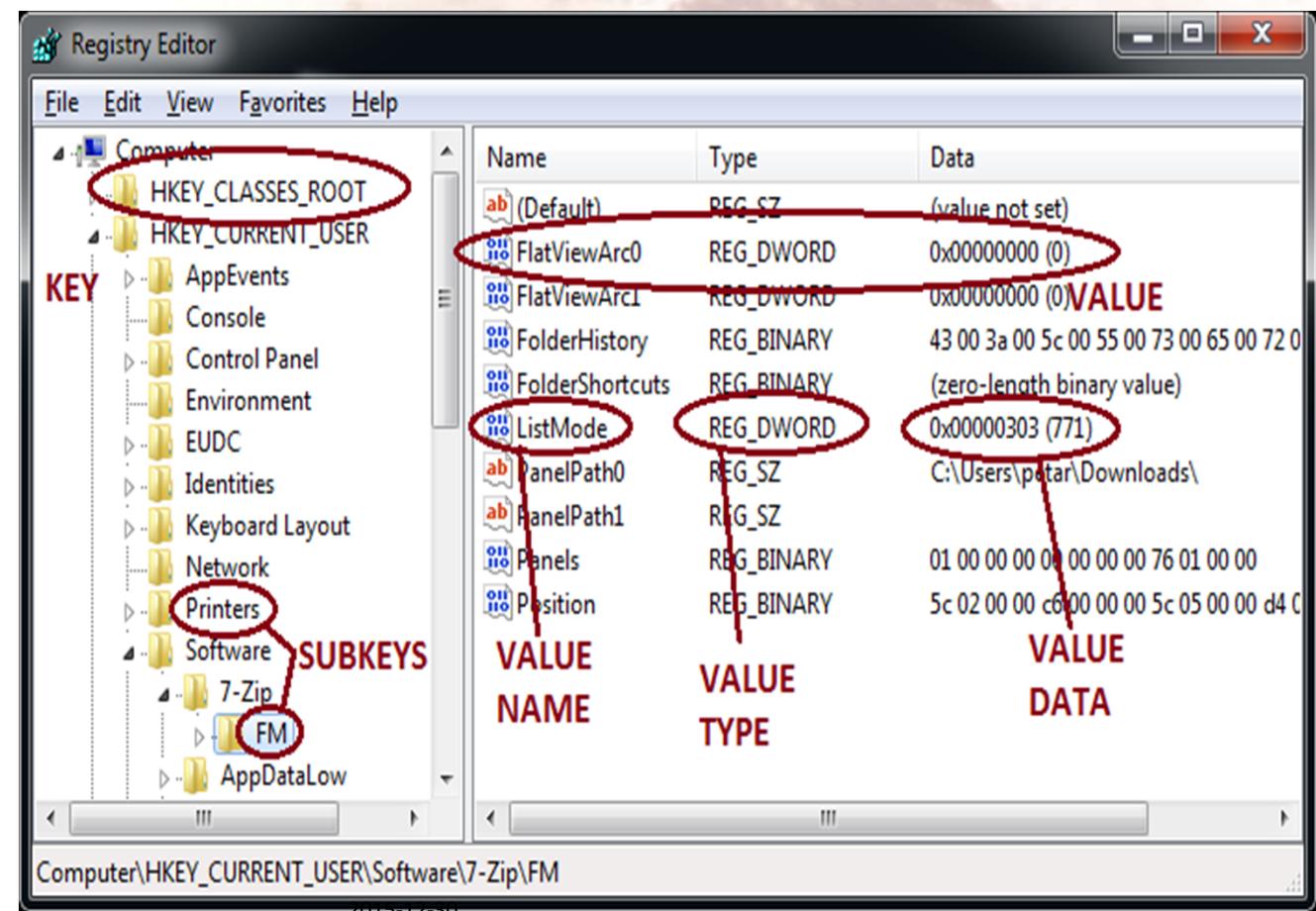
- Windows API (win32/win64):
 - [https://msdn.microsoft.com/en-us/library/windows/desktop/ms724875\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms724875(v=vs.85).aspx)
- .NET API (C# &friends):
 - [https://msdn.microsoft.com/en-us/library/microsoft.win32.registry\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/microsoft.win32.registry(v=vs.110).aspx)
- Windows Script Host: WshShell Object
 - [https://msdn.microsoft.com/en-us/library/aew9yb99\(v=vs.84\).aspx](https://msdn.microsoft.com/en-us/library/aew9yb99(v=vs.84).aspx)
- Windows PowerShell: razni Cmdlet-i
 - e.g. <https://technet.microsoft.com/en-us/library/ee176852.aspx>
- Ostali jezici :
 - mapiranje na C funkcije
 - većina jezika omogućava nekim mehanizmom
 - npr JNA za Javu, COM razred u PHP-u i sl.
 - preko “native” 3rd party biblioteka ili modula
 - npr. [Win32::Registry](#) ili [Win32::TieRegistry](#) na CPAN



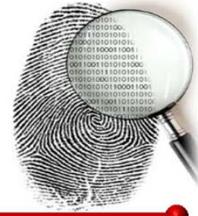
Logička organizacija



- podaci su pohranjeni u stablastu strukturu max. dubine 512 razina, koja se sastoji od:
- Ključeva (keys) i potključeva (subkeys)
- Vrijednosti (values)
 - ime vrijednosti (value name)
 - tip vrijednosti (value type)
 - podatci (value data)



Ključevi i vrijednosti



- Svaki čvor stabla je ključ ili potključ
 - ključ može sadržavati potključeve i vrijednosti (jednu ili više)
 - ime svakog potključa je jedinstveno unutar nadređenog ključa
 - ključ: vrhovi hijerarhija kao HKEY_CLASSES_ROOT, HKEY_CLASSES_USER
 - ostalo su potključevi
 - iako u literaturi se često koristi termin "key" u kontekstu roditelja bilo kojeg potključa te korištenje termina "root key" za vršne ključeve
- vrijednost (*value*) ima naziv (*name*), tip (*type*) i "vrijednost" (podatke, *data*)
 - Za ograničenja veličina vidi: [https://msdn.microsoft.com/en-us/library/windows/desktop/ms724872\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms724872(v=vs.85).aspx)
- TTip:
 - string (ASCII/Unicode),
 - DWORD (32-bit),
 - QWORD(64 bita), binary etc.
[https://msdn.microsoft.com/en-us/library/windows/desktop/ms724884\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms724884(v=vs.85).aspx)
- Preporuka:
 - duge binarne vrijednosti (>2,048 byte) pohraniti u datoteku,
 - a punu putanju datoteke u registry



Sadržaj registry-a



- Sistemski artefakti

- kreira i uređuje OS prvenstveno za vlastite potrebe
- aplikacije mogu vidjeti neke od vrijednosti, ovisno o ovlastima
- OS verzija, korisnici, grupe, liste pristupa (ACL), policies, putanje sistemskih datoteka, instaliran softver i komponente itd

- Korisnički artefakti

- kreiraju i uređuju aplikacije i alati, pristup ovisi o ovlastima

→ Zajednički (za sve korisnike)

◆ Konfiguracije instaliranih aplikacija (“for all users”, zahtjeva admin ovlasti)

→ Pojedinog korisnika

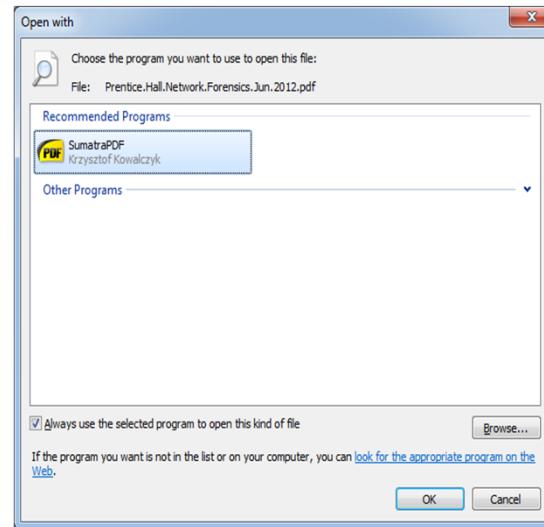
◆ recent documents, konfiguracija aplikacije “za mene” (npr web history za IE, veličina i pozicija prozora ili hash passworda za neku uslugu)



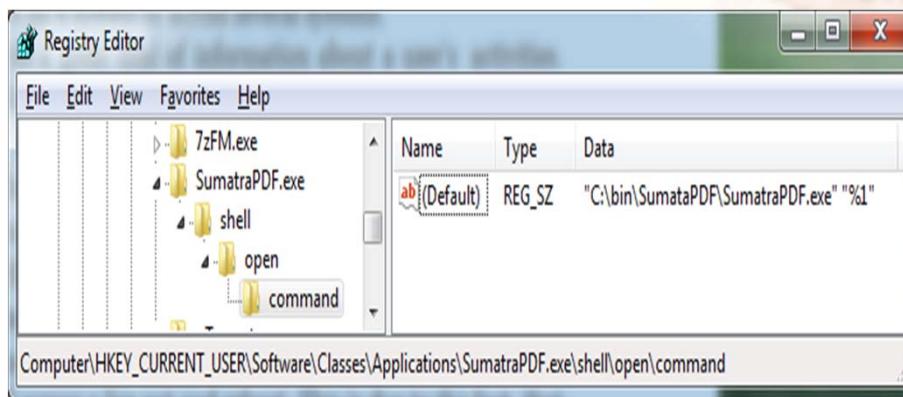
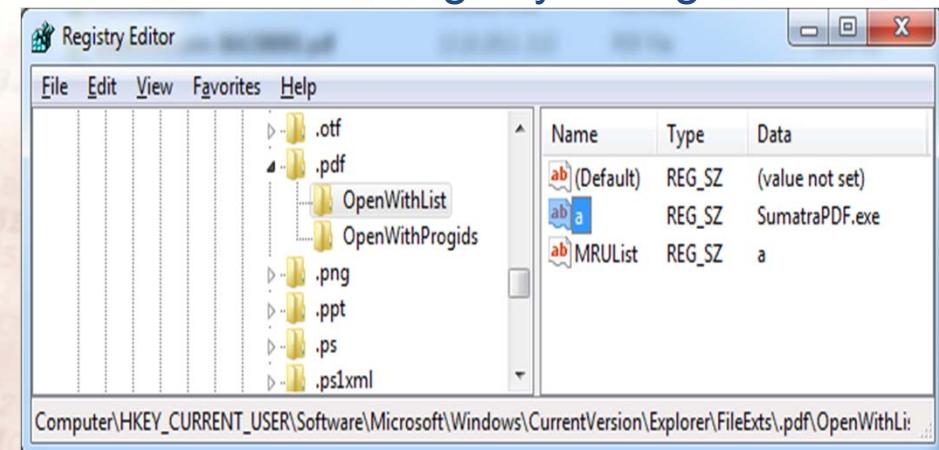
Sadržaj registry-a, primjer



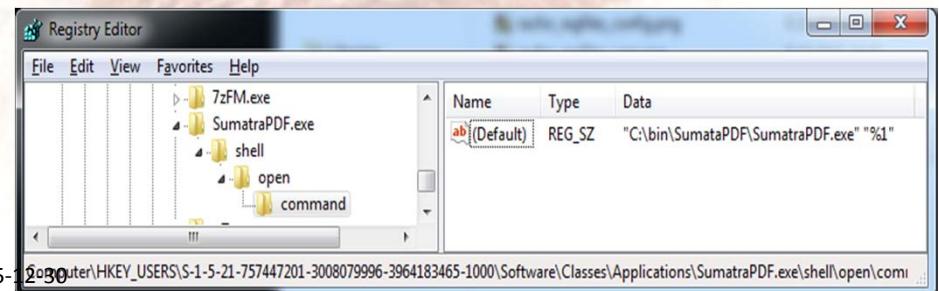
Trenutno prijavljeni korisnik je definirao program kojim se otvaraju datoteke određene ekstenzije



...što OS (win explorer) bilježi u registry za tog korisnika:



OS mora znati kako može pokrenuti taj program u ljestvi s ispravnim argumentima (zadanu vrijednost originalno je upisala instalacijska rutina programa),...

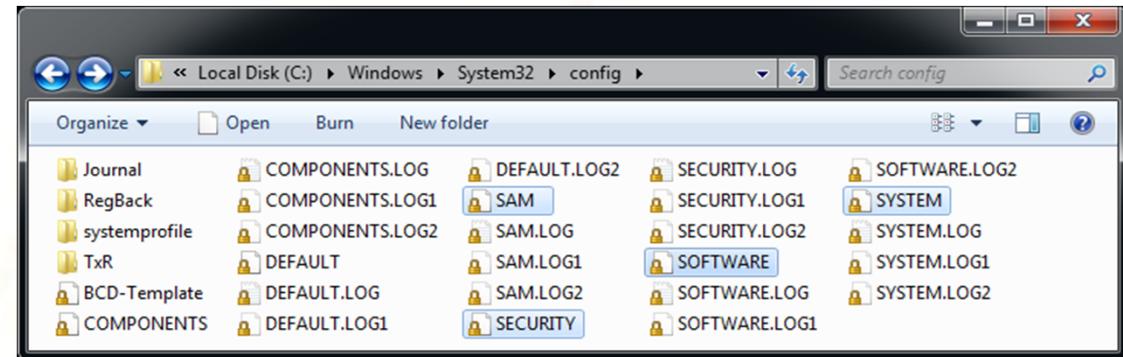


Fizička organizacija - datoteke (*hive files*)



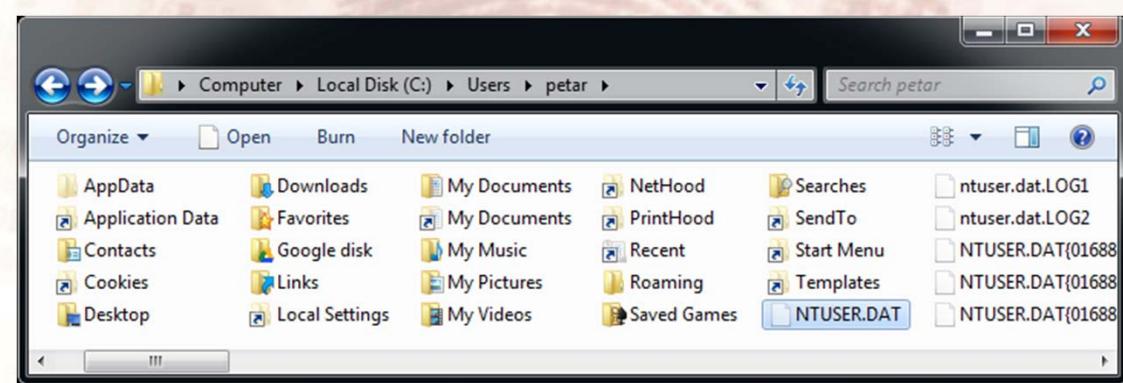
Na putanji <windows>\system32\config\

- SAM
- SECURITY
- SOFTWARE
- SYSTEM



Za svakog korisnika:

- NTUSER.DAT u korisničkoj mapi
za pregled datoteka u “folder options”
odznačiti
checkbox “hide protected operating
system files”
- USRClass.dat
u Local Settings\Application data\Microsoft
\Windows



dodatne datoteke mogu biti referencirane u vrijednostima registry-a

datoteke ↔ ključevi nisu 1:1!

npr. HKEY_CURRENT_USER su podaci iz HKEY_USERS/<ID trenutnog korisnika>
ovi podaci formirani su iz obje spomenute datoteke za korisnika



Fizička organizacija - *hives vs. hive files*

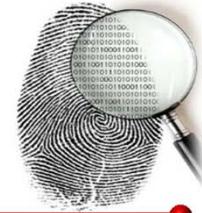


Hive Registry Path	Hive File Path
HKEY_LOCAL_MACHINE \SYSTEM	\winnt\system32\config\system
HKEY_LOCAL_MACHINE \SAM	\winnt\system32\config\sam
HKEY_LOCAL_MACHINE \SECURITY	\winnt\system32\config\security
HKEY_LOCAL_MACHINE \SOFTWARE	\winnt\system32\config\software
HKEY_LOCAL_MACHINE \HARDWARE	Volatile hive
HKEY_LOCAL_MACHINE \SYSTEM \Clone	Volatile hive
HKEY_USERS \UserProfile	Profile; usually under \winnt\profiles\users
HKEY_USERS.DEFAULT	\winnt\system32\config\default

**Mark Russinovich, “Inside the Registry”, Windows NT Magazine, available at
<https://technet.microsoft.com/en-us/library/cc750583.aspx>**



Fizička organizacija - *bins, cells*



- svaka hive datoteka se sastoji od blokova veličine 4KiB (tzv. bins)
 - olakšavajuća okolnost: $4\text{Ki} = 2^{12} = (2^4)^3 = 1000_{(16)}$
- svaki blok (osim prvog) počinje "magic" nizom 68 62 69 6E 00
 - (ASCII za "hbin")
- Zapis u bloku
 - tzv. ćelije, *cells*
 - odnosi se na ključ
 - ili vrijednost
- zapravo je više vrsta zapisa,
 - detaljnije na
 - <https://technet.microsoft.com/en-us/library/cc750583.aspx>

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000FC0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000FD0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000FE0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000FF0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001000	68 62 69 6E 00 00 00 00 10 00 00 00 00 00 00 00
00001010	00 00 00 00 F0 34 43 B1 29 00 D1 01 00 00 00 00
00001020	78 FF FF FF 6E 6B 2C 00 00 17 71 99 29 00 D1 01
00001030	x nk,...q... .N.
00001040	00 00 00 00 06 00 00 0B 00 00 00 01 00 00 00
00001050	20 20 01 00 68 02 00 80 00 00 00 FF FF FF FF
00001060	..h..€....
00001070	00 00 00 FF FF FF FF 20 00 00 00 00 00 00 00
00001080	..
00001FF0	A8 29 07 00 43 6F 6E 74 F8 FF FF FF 80 50 06 00
00002000	hbin.....
00002010	68 62 69 6E 00 10 00 00 00 10 00 00 00 00 00
00002020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00002030	00 00 00 00 48 0F 00 00 02 00 00 00 00 00 00 00
00002040	nk <...Dí.
00002050	00 00 00 00 48 0F 00 00 02 00 00 00 00 00 00 00
00002060	Pž... .T..
00002070	00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00
00002080

načelno zapisi ne prelaze granice bloka (bin-a)
nego je jedan zapis sadržan unutar bloka



Format zapisa o ključu - key cell format



poz	vel	opis
0	4	veličina zapisa
4	2	NodeID
6	2	tip čvora
8	8	LastWriteTime (kasnije više o tome)
20	4	pomak od roditelja

24	4	Broj potključeva
32	4	pomak zapisima o potključevima
36	4	broj vrijednosti
44	4	pomak prema listi vrijednosti
48	4	pomak prema sigurnosnom zapisu
76	2	duljina imena ključa

(lista nije potpuna, samo navodi forenzički najzanimljivije elemente)

Nakon ove strukture slijedi ime ključa (duljine definirane posljednjim poljem) te eventualna popuna (*padding*) do “okrugle” veličine

veličina zapisa = ovih 80 bajtova + duljina imena + padding





Korisni tragovi u *key cell*-u

LastWriteTime

- 64 bitna FILETIME struktura
- OS vodi evidenciju (ne upisuje aplikacija/korisnik)
- broj 100-nanosekundnih intervala od ponoći 1.1.1601.
 ⑨ Od ponoći 1.1.1601

Veličina

- za aktivne zapise negativna vrijednost prave veličine zapisa
 ⑨ kao signed integer
 - 4-bajtni dvojni komplement,
 npr. za zapis veličine 102 bajta je DWORD_MAX-101
- brisanje ključa = **logičko brisanje**
 ⑨ postavljanjem ove vrijednosti na pozitivan broj
 - dodatno prostor ćelije postaje neallocirani prostor registry-a!



Value cell format



Nema timestamp polja!

Vrijedi li za veličinu slično
kao kod keycell strukture?
Isprobati za vježbu...

poz	vel	opis
0	4	veličina (kao negativan broj)
4	2	NodeID
6	2	Duljina naziva vrijednosti
8	4	Duljina podatka
12	4	Pomak podatka
16	4	Tip podatka

(not an exhaustive list)



Alati



Bitne podjele: online vs. offline,
API vs. gotovi alati,
free vs. proprietary

Pristup živom (online) registry-u

- važan u incident response scenarijima
- ograničen osnovnim win32 API:
 - obično pristup samo logičkoj strukturi

Pristup offline registry-u

- pristup (forenzičkoj) kopiji datoteka registry-a
- potraga za poznatim fenomenima
 - (pobrisani ključevi, konkretni ključevi i vrijednosti, nekonzistencije, malware signatures itd.)

Best friends: Google & Github





Alati, nastavak

Cjeloviti alati

→ mali specijalizirani alati (npr. perl skripte)

• ili dijelovi cjelokupnih forenzičkih rješenja

→ *suites* i *toolkits*, npr. FTK, enCase, Sleuth itd.

→ često plugin arhitektura:

• laka nadogradnja komponentama

• temeljenim na novostečenim spoznajama o sadržajima u registry-u

→ nove aplikacije, novo pronađeni tragovi zločudnog koda i sl.

API

→ Za izradu novih alata po potrebi

→ live analiza: wrapperi oko win32 API-a

→ analiza offline datoteka:

• parseri datoteka,

→ predstavljaju podatke na organiziran način

→ npr. kroz objektni model registry artefakata



Pristup živom registry-u



- Registry editor (regedit.exe)
 - je dio svake Windows instalacije
- Reg – alat za poziv znakovnog korisničkog sučelja
 - koristan za uključivanje u skripte
 - Reg <operation> [key] (todo: dodati ostatak)
- Ranije spomenuti wrapperi oko win32 API poziva, npr:
 - Win32::TieRegistry (Perl)
 - _winreg/winreg (Python)
 - WMI (wrapperi u .NET, MFC itd)
 - Windows Script Host
 - ...



Pristup hladnom registryu: regscan.pl



- perl skripta uključena u CPAN modul Parse::Win32Registry
- ispisuje postojeće zapise
s pripadajućim vremenom izmjene (ako postoji)
- perlscan.pl --help za više

Primjer:

```
petar@asus$ regscan.pl NTUSER.DAT | head -n 10
0x1020 CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} [2015-09-02T06:07:01Z]
0x10a8 CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft [2015-09-02T06:07:01Z]
0x1108 (subkey list entry)
0x1120 (subkey list entry)
0x1130 IE5_UA_Backup_Flag (REG_SZ) = 5.0
0x1160 CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software [2015-09-02T06:07:01Z]
0x11b8 (unidentified entry)
0x11c8 CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Policies [2015-05-25T20:53:16Z]
0x1220 (unidentified entry)
0x1228 (unidentified entry)
```



Pristup hladnom registryu: RegRipper



→ <https://github.com/keydet89/RegRipper2.8/>

→ Perl command-line alat

→ aktivno održavanje: posljednja izmjena (izmjena jednog plugin-a) prije >30 dana

→ jednostavna plugin arhitektura:

↗ mapa plugins

↗ 1 plugin = 1 logička funkcionalnost

↗ 1 plugin = 1 perl skripta = 1 “pluginmain” procedura

↗ rujan 2015.: 325 pluginova

↗ bundle datoteke: all/security/sam/ntuser/... (sve razumne pretrage za odabranu datoteku)

→ dostupni i perl2exe generirani PE-ovi rip.exe i rr.exe (GUI za pokretanje) za Windows bez Perl-a

→ koristi se kao dio nekoliko forenzičkih toolset-a

⑨ Revealer Toolkit, SANS, PlainSight itd

→ perl rip.pl -help for more





RegRipper primer

```
petar@asus$ perl rip.pl -r ~/fer/racfor/registry/myfiles/petar/NTUSER.DAT -p winlogon_u
Launching winlogon_u v.20130425
winlogon_u v.20130425
(NTUSER.DAT) Get values from the user's WinLogon key

Software\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Sun May 31 09:16:58 2015 (UTC)
FirstLogon = 0
ParseAutoexec = 1
BuildNumber = 7601
ExcludeProfileDirs = AppData\Local;AppData\LocalLow;$Recycle.Bin

Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon not found.

Analysis Tip: Existence of RunGrpConv = 1 value may indicate that the
system had been infected with Bredolab (Symantec). Also, check the
contents of a "shell" value - should only include Explorer.exe, if
it exists.

petar@asus$
```



Pristup hladnom registryu: regslack.pl



- perl skripta za otkrivanje logički pobrisanih ključeva i neallociranog prostora
 - <https://github.com/keydet89/Tools/>
 - originalni autori regslack i regripper skripti su različite osobe
 - ali trenutno se oba alata uz neke druge mogu naći u github repozitorijima Harlana Carveya
 - forenzičara i autora više knjiga o Windows forenzici
- Example:

```
petar@asus$ perl regslack.pl ../../win7IE10/NTUSER.DAT | head -26
"\?\?\C:\Users\IEUser\ntuser.dat"
[Tue Oct  6 11:25:23 2015]

### Deleted Key ###

CMI-CreateHive{6A1C4018-979D-4291-A7DC-
7AED1C75B67C}\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\Drives\Volume{a509785a-
75af-11e4-b72d-806e6f6e6963}\Current Media
Offset: 0x85e30 [Tue Oct  6 11:24:57 2015]
Number of values: 0
```



regslack.pl (nastavak)



```
Recovered 1 keys and 0 values: #0 keys from allocated space.
```

```
Rejected 0 keys and 0 values.
```

```
### Unallocated Space ###
```

```
Offset 0x71f70 - 0x71f90:
```

```
20 00 00 00 76 6b 07 00 04 00 00 80 00 00 00 00 ....vk.....  
04 00 00 00 01 00 4c 73 4c 69 76 65 20 46 53 00 .....LsLive.FS.
```

```
Offset 0x72e08 - 0x72e18:
```

```
10 00 00 00 50 4f 08 00 88 50 08 00 70 51 08 00 ....P0...P..pQ..
```

```
Offset 0x73cf8 - 0x73d08:
```

```
10 00 00 00 6c 66 01 00 90 2c 07 00 66 38 2d 31 ....lf....f8-1
```

```
Offset 0x754e8 - 0x75500:
```

```
(...)
```





ComFor.zesoi.fer.hr
ComFor@zesoi.fer.hr

