Windows Forensic 101

FORKRIPT TALKS
Badan Siber dan Sandi Negara
22 Juli 2021

Digit Oktavianto
@digitoktav
https://threathunting.id

T1033 : System Owner/User Discovery

- **Infosec Consulting Manager at Mitra Integrasi Informatika**
- **Co-Founder BlueTeam.ID (https://blueteam.id)**
- **Born to be DFIR Team**
- **Community Lead @ Cyber Defense Community Indonesia**
- **Member of Indonesia Honeynet Project**
- **Opreker and Researcher**
- **{GCIH | GMON | GCFE | GICSP | CEH | CSA | ECSA | ECIH | CHFI | CTIA | ECSS} Certifications Holder**

Agenda

- Windows Forensic Analysis Fundamental
- Forensic Artifacts
- Windows Process genealogy
- Windows Registry
- Windows Artifacts

Analysis Process in Cyber Investigation

- Understanding OS, Applications, and Investigation
- Evidence Created
  - User Action
  - System Action
- Problem Solving Skills
- Require Analysis
  - Not just data extraction
  - 5W, 1H

Windows Forensic Analysis Fundamental

- Proper analysis is not simply about :
  - Finding artifacts, Documents, Pictures, Video, Executable Files
  - Recovering Deleted Data
  - Reconstruct Email Communication
  - Checking the entries from Event Log
- Analysis require understanding of how the evidence can help the forensic investigator to answer the question, like :
  - Browsing history from user and downloaded files from the browser forensic
  - Opening Download directory
  - Executing the files just downloaded
  - Network communication to external domain and ip
  - ➢ **This is analysis…. Correlate the information that you get with your hypotheses, and answering the question what actually happened on that machine**
- Focus on which question need to be answered :
  - Build solid timeline analysis
  - Focus on detailing facts based on your finding

Forensic Artifacts

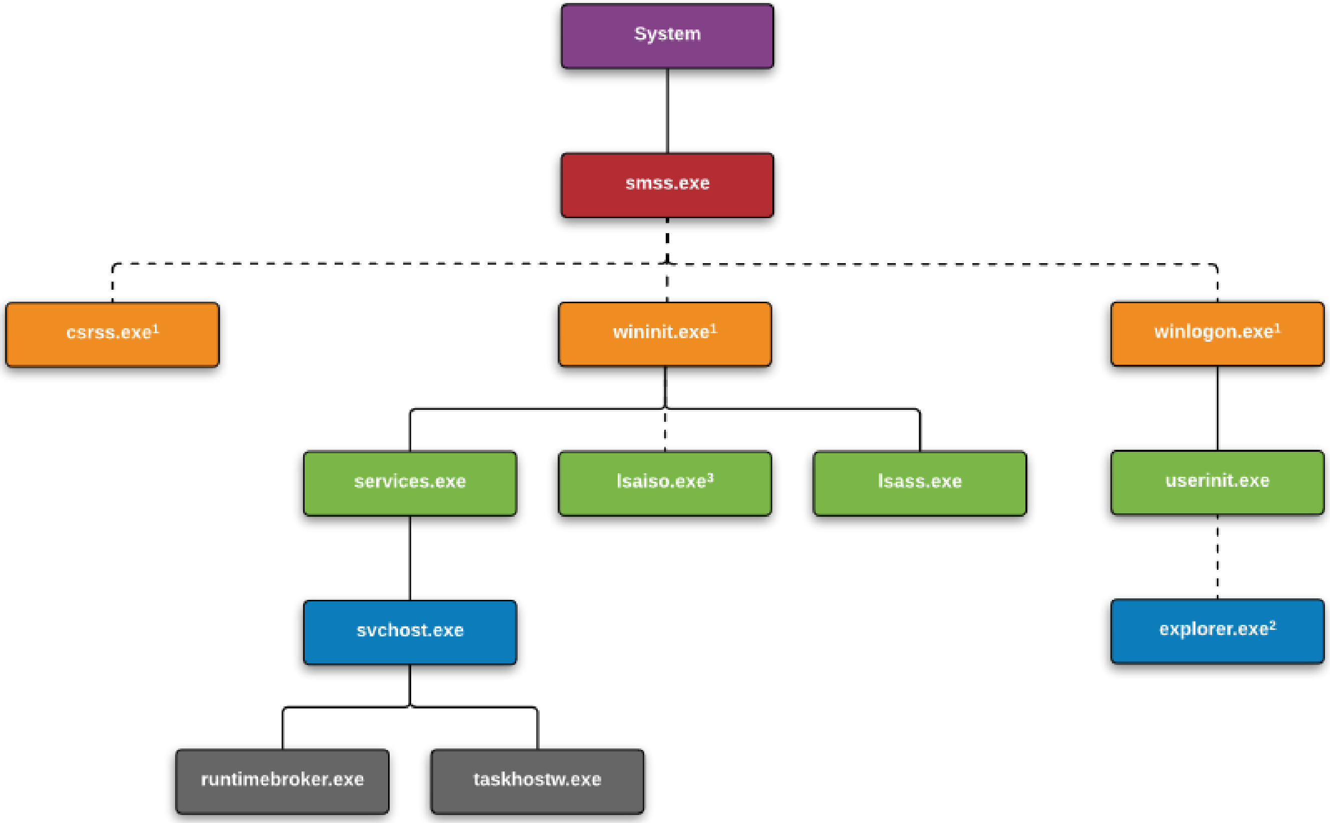
Volatile Artifact

- Memory
- Process
- Network Related Artficats
- etc

Non-Volatile Artifacts

- Windows File System
- Windows Registry Hive
- Windows Event Log
- Prefetch
- Volume Shadow Copy
- etc

Windows Process Genealogy (13cubed)



[1] Created by an instance of **smss.exe** that exits, so analysis tools usually do not provide the parent process name.

[2] Created by an instance of **userinit.exe** that exits, so analysis tools usually do not provide the parent process name.

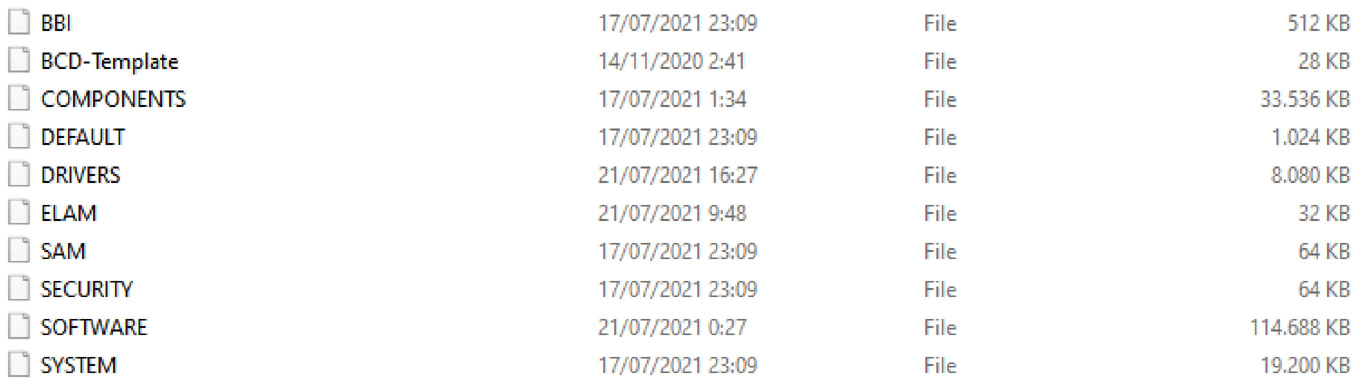
[3] Present only when **Credential Guard** is enabled. Functionality of lsass.exe is split between itself and this process.

Windows Registry

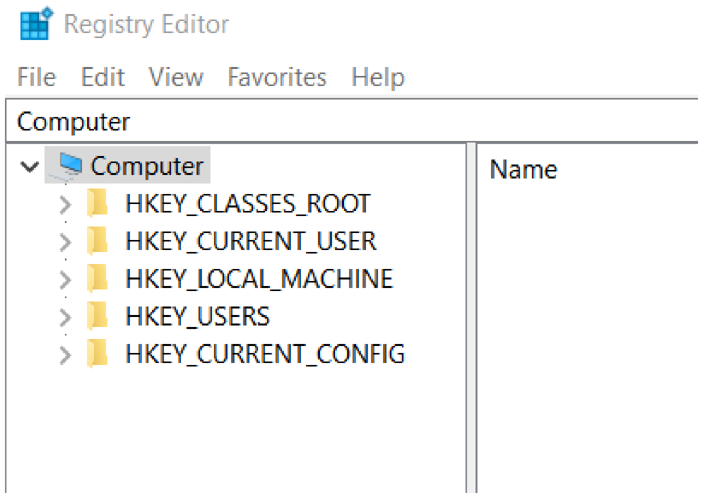
- Central database of Windows
- The database contains most of the settings for Windows, Programs,hardware and users.
- Such as, profiles for each user, the applications installed on the computer , what hardware exist on the system and the last shut down time of computer, etc

Windows Registry

- C:\Windows\System32\config



BBI	17/07/2021 23:09	File	512 KB
BCD-Template	14/11/2020 2:41	File	28 KB
COMPONENTS	17/07/2021 1:34	File	33.536 KB
DEFAULT	17/07/2021 23:09	File	1.024 KB
DRIVERS	21/07/2021 16:27	File	8.080 KB
ELAM	21/07/2021 9:48	File	32 KB
SAM	17/07/2021 23:09	File	64 KB
SECURITY	17/07/2021 23:09	File	64 KB
SOFTWARE	21/07/2021 0:27	File	114.688 KB
SYSTEM	17/07/2021 23:09	File	19.200 KB



Registry Editor

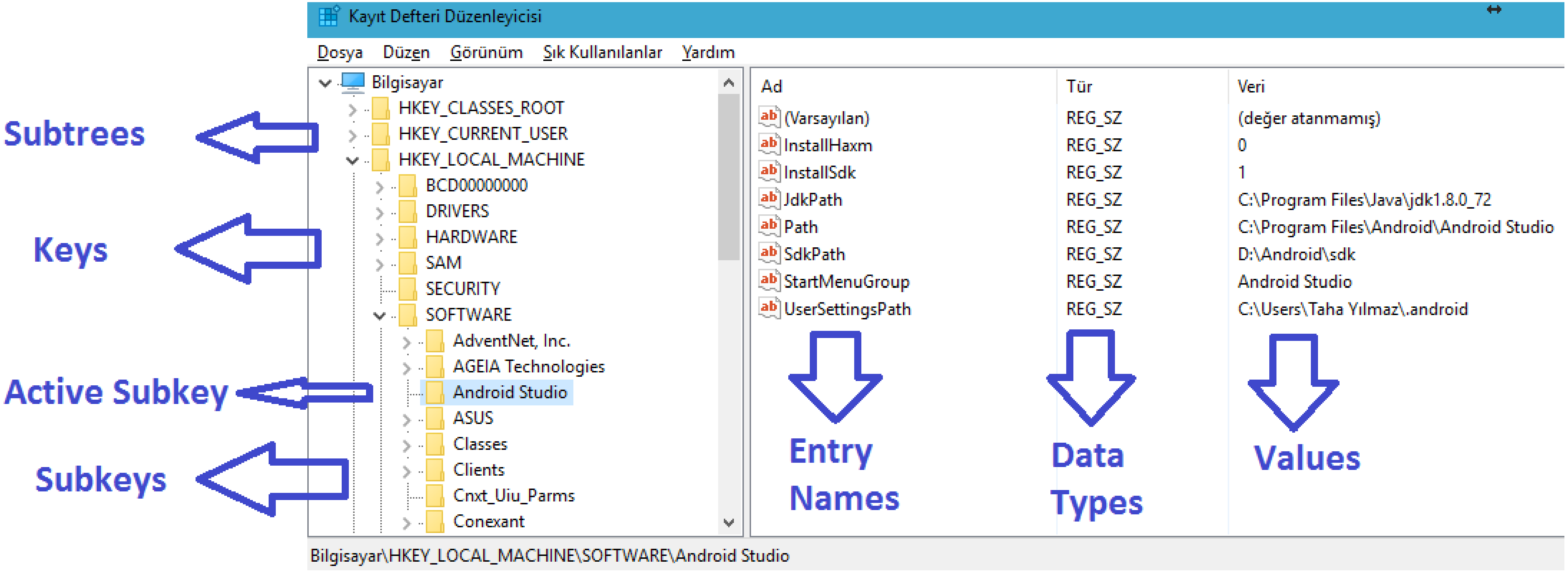
Computer

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG

Windows Registry

- HKCR - Contains information about the correct program opens when executing a file with Windows Explorer.
- HKCU - Contains the profile about the user that is logged on.
- HKLM - Contains system-wide hardware settings and configuration information.
- HKU - Contains all user profiles that exist on the system.
  - Also contains information about the type of hardware installed , default settings of softwares and desktop configurations. These informations is used for all users who log on to this computer.
- HKCC - Contains information about the hardware profile used by the computer start up.

Windows Registry



- Bilgisayar
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
    - BCD00000000
    - DRIVERS
    - HARDWARE
    - SAM
    - SECURITY
    - SOFTWARE
      - AdventNet, Inc.
      - AGEIA Technologies
      - Android Studio
      - ASUS
      - Classes
      - Clients
      - Cnxt_Uiu_Parms
      - Conexant

Ad	Tür	Veri
(Varsayılan)	REG_SZ	(değer atanmamış)
InstallHaxm	REG_SZ	0
InstallSdk	REG_SZ	1
JdkPath	REG_SZ	C:\Program Files\Java\jdk1.8.0_72
Path	REG_SZ	C:\Program Files\Android\Android Studio
SdkPath	REG_SZ	D:\Android\sdk
StartMenuGroup	REG_SZ	Android Studio
UserSettingsPath	REG_SZ	C:\Users\Taha Yılmaz\.android

Bilgisayar\HKEY_LOCAL_MACHINE\SOFTWARE\Android Studio

Subtrees

Keys

Active Subkey

Subkeys

Entry Names

Data Types

Values

Windows Forensic 101

- Windows Artifacts Analysis based on Evidence of :
  - Program Execution
  - Deleted File or File Knowledge
  - Network Activity / Physical Location
  - File / Folder opening
  - Account usage
  - External Device / USB Usage
  - Browser usage
  - File Download

Windows Artifact – Program Execution

- UserAssist
- Last-VisitedMRU
- RecentApps
- Shimcache
- Background / Desktop Activity Moderator (BAM / DAM)
- Amcache
- Jump Lists
- System Resource usage Monitor
  - Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.
- Prefetch
- Windows 10 Timeline (Win + TAB)

NTUSER.DAT Hive

SYSTEM Hive

Windows Artifact – Deleted File or File Knowledge

- Search - WordWheelQuery
- Last-VisitedMRU

NTUSER.DAT Hive

- Thumbscache
  - Thumbnails of pictures, office documents, and folders exist in a database called the thumbcache. Each user will have their own database based on the thumbnail sizes viewed by the user (small, medium, large, and extra-larger)
- Thumbsdb
  - Hidden file in directory where images on machine exist stored in a smaller thumbnail graphics. thumbs.db catalogs pictures in a folder and stores a copy of the thumbnail even if the pictures were deleted.
- Windows Recycle Bin
- IE|Edge file://

Windows Artifact – Network Activity / Physical Location

- Timezone (SYSTEM Hive)
- Cookies (Browser)
- Network History (SOFTWARE Hive)
- WLAN Event Log
  - Microsoft-Windows-WLAN-AutoConfig Operational.evtx
  - 11000 – Wireless network association started
  - 8001 – Successful connection to wireless network
  - 8002 – Failed connection to wireless network
  - 8003 – Disconnect from wireless network
  - 6100 – Network diagnostics (System log)
- Browser Search Terms
- System Resource Usage Monitor (SRUM) (SOFTWARE Hive)
  - Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.

Windows Artifact – File / Folder Opening

- Open / Save MRU
- ShellBags
- Last-Visited MRU
- Recent Files
- Shortcut (LNK) Files
- IE|Edge File://
- Jump Lists
- Prefetch
- Office Recent Files

Windows Artifact – Account Usage

- **Last Login (SAM Hive)**
- **Last Password Change (SAM Hive)**
- **Logon Types**
  - Success Logon Event ID 4624 in Windows Event Log
  - LogonType from 2 – 13 from Windows Event Log
- **RDP usage**
  - Windows Event Log Security.evtx
  - Event ID 4778 – Session Connected/Reconnected
  - Event ID 4779 – Session Disconnected
- **Services Event**
  - Windows Event Log System.evtx and Security.evtx
  - 034 – Service crashed unexpectedly
  - 7035 – Service sent a Start/Stop control
  - 7036 – Service started or stopped
  - 7040 – Start type changed (Boot | On Request | Disabled)
  - 7045 – A service was installed on the system (Win2008R2+)
  - 4697 – A service was installed on the system (from Security log)
- **Authentication Events**
  - Windows Event Log Security.evtx
  - Event ID Codes (NTLM protocol)
  - 4776: Successful/Failed account authentication

  Event ID Codes (Kerberos protocol)
  - 4768: Ticket Granting Ticket was granted (successful logon)
  - 4769: Service Ticket requested (access to server resource)
  - 4771: Pre-authentication failed (failed logon)
- **Success / Fail Logons**
  - 4624 – Successful Logon
  - 4625 – Failed Logon
  - 4634 | 4647 – Successful Logoff
  - 4648 – Logon using explicit credentials (Runas)
  - 4672 – Account logon with superuser rights (Administrator)
  - 4720 – An account was created

Windows Artifact – External Device / USB Usage

- Key Identification (SYSTEM Hive)
  - SYSTEM\CurrentControlSet\Enum\USBSTOR
  - SYSTEM\CurrentControlSet\Enum\USB
- First / Last Times Connected
  - C:\Windows\inf\setupapi.dev.log
- User
  - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
- Pnp (Plug and Play) Events
  - System.evtx Windows Event Log
  - Event ID: 20001 – Plug and Play driver install attempted
  - Event ID 20001 – Timestamp, Device information, Device serial number, Status (0 = no errors)
- Volume Serial number
  - SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt
- Drive Letter and Volume Name
- Shortcut (LNK) Files

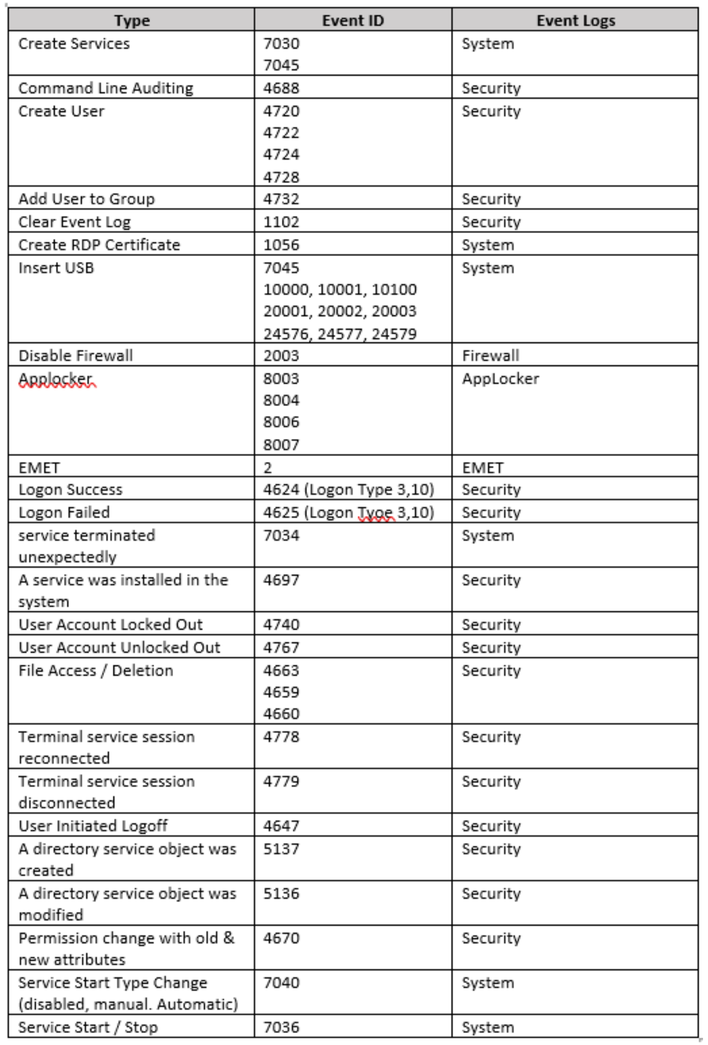
Windows Artifact – Browser Usage

- History
- Cache
- Cookies
- Session Restore
- Google Analytics Cookies

Windows Artifact – File Downloaded

- Open / Save MRU
- Email Attachments
- Skype History
- Browser Artifacts
- Downloads
  - Firefox and IE has a built-in download manager application which keeps a history of every file downloaded by the user. This browser artifact can provide excellent information about what sites a user has been visiting and what kinds of files they have been downloading from them.
  - Firefox: Win7/8/10:
  - %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite
  - Internet Explorer: IE8-9: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\
  - Internet Explorer: IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV*.dat
- AD Zone Identifier
  - Starting with XP SP2 when files are downloaded from the “Internet Zone” via a browser to a NTFS volume, an alternate data stream is added to the file. The alternate data stream is named “Zone.Identifier.”

Critical Windows Log Review for Forensic Investigation



Type	Event ID	Event Logs
Create Services	7030 7045	System
Command Line Auditing	4688	Security
Create User	4720 4722 4724 4728	Security
Add User to Group	4732	Security
Clear Event Log	1102	Security
Create RDP Certificate	1056	System
Insert USB	7045 10000, 10001, 10100 20001, 20002, 20003 24576, 24577, 24579	System
Disable Firewall	2003	Firewall
Applocker	8003 8004 8006 8007	AppLocker
EMET	2	EMET
Logon Success	4624 (Logon Type 3,10)	Security
Logon Failed	4625 (Logon Type 3,10)	Security
service terminated unexpectedly	7034	System
A service was installed in the system	4697	Security
User Account Locked Out	4740	Security
User Account Unlocked Out	4767	Security
File Access / Deletion	4663 4659 4660	Security
Terminal service session reconnected	4778	Security
Terminal service session disconnected	4779	Security
User Initiated Logoff	4647	Security
A directory service object was created	5137	Security
A directory service object was modified	5136	Security
Permission change with old & new attributes	4670	Security
Service Start Type Change (disabled, manual. Automatic)	7040	System
Service Start / Stop	7036	System

https://medium.com/mii-cybersec/log-analysis-for-digital-forensic-investigation-e4a00f5a5c09

Critical Windows Log Review Quick Summary

- Service Created, New Service Installed, Service Start, Service Stop : Usually related on Persistence Mechanism
- User Account Added, User Account Modified, Add User to Group : also related on persistence mechanism by attacker
- Clear Event Log : Usually related on Covering the Tracks
- Disable Firewall, Stop Security Services (such as AV, HIPS, other Endpoint Protection) : Related to Attacker activity for further movement
- Terminal Service Session : Related to Remote Access Activity user
- USB Log : Case incident like data theft, fraud, etc maybe need this kind of USB log to identify USB Storage access into system

Windows Event Log for Forensic Investigation Reference

- https://www.malwarearchaeology.com/cheat-sheets/

The URL above provides a variety of detailed information about the intricacies of the Log on the Windows Platform. You can get very valuable information there. The website author also includes a mapping between Windows Log with MITRE ATT&CK Framework where the ATT&CK is a Framework that studies TTPs (Tactic, Technique, and Procedure) from threat actors, so this makes it easier for investigators to understand how the thinking about the patterns are commonly used by Threat Actor, and where the source log / log location can be used as a reference for analyzing TTPs used by threat Actors

- https://www.ultimatewindowssecurity.com/

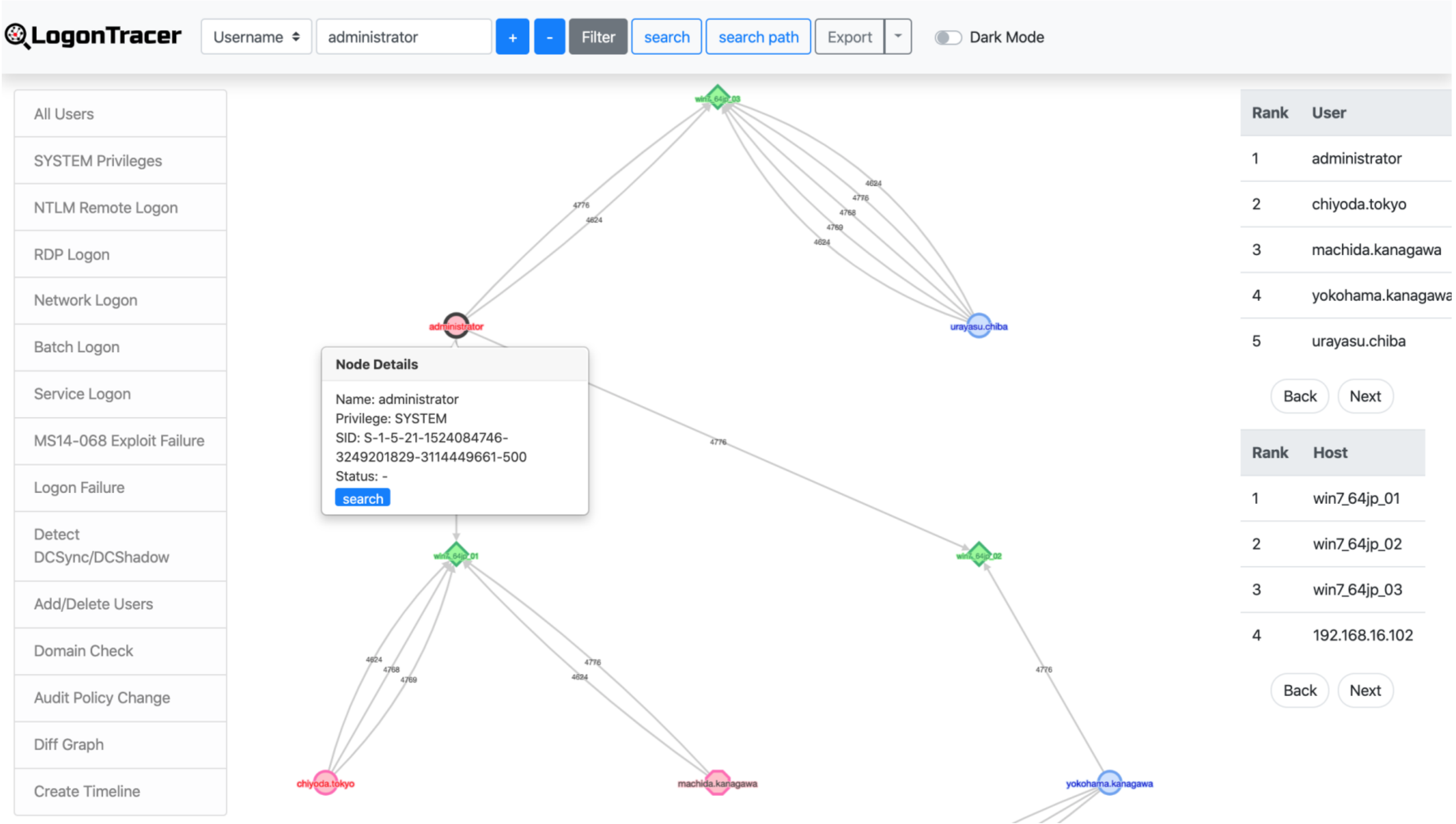
The above website is one of the author's reference sources related to Event ID Widows. As we all know, there are a lot of Windows Event IDs and types for each of these Event IDs, so for those of you who have difficulty memorizing or often forgot for some Windows Event IDs that may not appear in the common log in the Windows Event Viewer, you can use that website as reference. The website above can be used as a reference to learn in more detail about the Windows Event ID and also they provides information in the form of a Cheat Sheet to pay attention to some Windows Event IDs that often correlate with the activities of threat actors / security incidents.

- https://www.jpcert.or.jp/english/pub/sr/ir_research.html

The URL above is the research from the JP CERT Team (Japan Computer Emergency Response Team) regarding the detection of Lateral Movement from Threat Actors using Event Logs. The research published by JP CERT is very interesting, especially focusing on the use of tools and TTPs used by threat actors when conducting Lateral Movement

JP CERt Tools Logon Tracer

- https://github.com/JPCERTCC/LogonTracer



Node Details

Name: administrator
Privilege: SYSTEM
SID: S-1-5-21-1524084746-3249201829-3114449661-500
Status: -
search

Rank	User
1	administrator
2	chiyoda.tokyo
3	machida.kanagawa
4	yokohama.kanagawa
5	urayasu.chiba

Rank	Host
1	win7_64jp_01
2	win7_64jp_02
3	win7_64jp_03
4	192.168.16.102

Windows Forensic Tools

- Evidence Acquisition
  - FTK Imager
  - Belkasoft RAM Capturer
  - KAPE
  - Brimorlabs
  - Comae
- Evidence Analysis
  - Arsenal Image Mounter
  - Autopsy / The Slueth Kit
  - Eric Zimmerman Tools FTW!!! https://ericzimmerman.github.io
  - Sysinternals Tools
  - Plaso (Log2Timeline)
  - OSForensics (Comemrcial)
  - Volatility
  - Wireshark
  - Event Log Explorer
  - Nirsoft Tools https://www.nirsoft.net/
  - Didier Steven's Tools https://blog.didierstevens.com/my-software/
  - All Useful Tools in SANS SIFT Workstation VM!

Reference

- 13Cubed Video Series on Youtube (https://www.youtube.com/channel/UCy8ntxFEudOCRZYT1f7ya9Q)
- Professor Ali Hadi https://www.ashemery.com/
- DFIR Diva https://dfirdiva.com/
- https://thisweekin4n6.com

THANK YOU
Q & A