

레지스트리란? -> 윈도우에서 컴퓨터 하드웨어, 응용프로그램, 서비스, 보안 및 사용자들에 대한 세팅 등 전반적인 설정을 담는 중앙 계층형 데이터베이스

레지스트리 루트키

1. HKEY_CLASSES_ROOT

- 파일 확장자명과 이에 연결되는 Application 정보, COM 객체 등록 정보

2. HKEY_CURRENT_USER

- 현재 시스템 상 로그인된 사용자 정보(C:\Users\<username>\NTUSER.DAT)
- HKEY_USERS에 대해 우선권을 가짐

3. HKEY_LOCAL_MACHINE

- 시스템 전체 H/W, S/W 정보, 드라이버나 환경 설정 사항

1) HKEY_LOCAL_MACHINE\HARDWARE

- 부팅시 감지된 H/W와 이의 드라이버 매핑 정보 (장치관리자)
- 시스템 상 파일로 존재 X, 메모리 상 휘발성 정보로만 존재

2) HKEY_LOCAL_MACHINE\SAM

- 사용자 PW, 소속 그룹, 도메인 정보 등 로컬 계정 정보 및 그룹정보 저장
- 컴퓨터가 도메인 컨트롤러일 경우, 액티브 디렉토리(AD서버)에 도메인 계정/그룹 정보 저장

3) HKEY_LOCAL_MACHINE\SECURITY

- 시스템 범위의 보안 정책, 사용자 권리 할당 정보

4) HKEY_LOCAL_MACHINE\SOFTWARE

- 시스템 범위의 S/W 목록, 환경설정 정보(Application의 이름, 경로 등)

5) HKEY_LOCAL_MACHINE\SYSTEM

- 시스템 부팅 시 필요한 시스템 환경 설정 정보(디바이스 드라이버, 시작 서비스 목록 등)
- 부팅 복사본 생성 및 백업

4. HKEY_USERS

- 시스템 상 모든 계정/그룹에 관한 정보 (서브키가 HKCU와 동일)

5. HKEY_CURRENT_CONFIG

- 시스템 시작 시 사용되는 H/W 정보
- 부팅 시 생성, Disk 적재 X

6. HKEY_PERFORMANCE_DATA

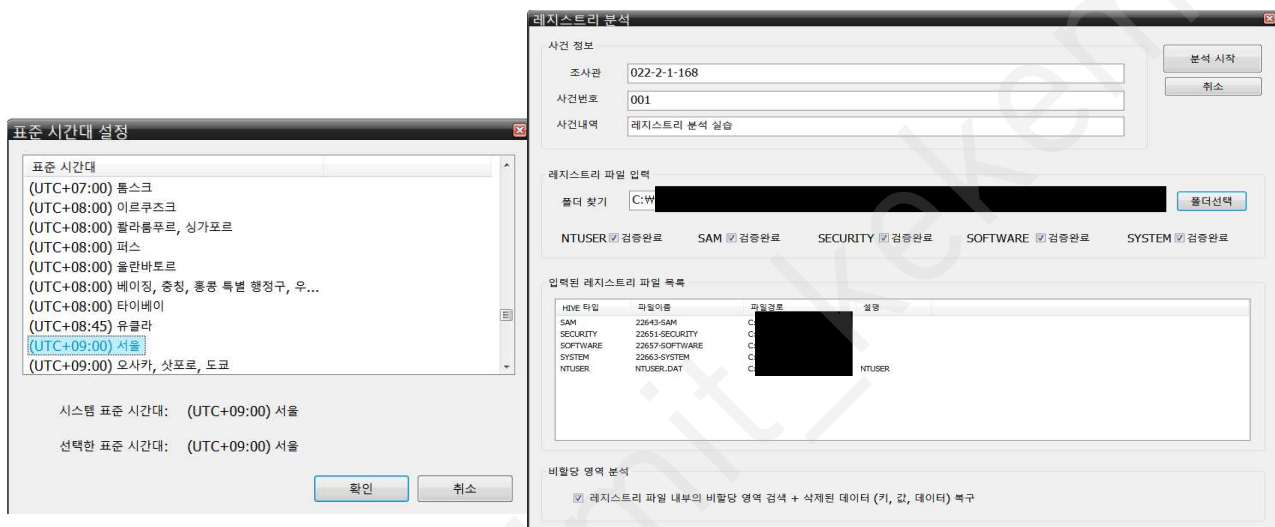
- 런타임 성능 정보
- 레지스트리 편집기에서 보이지 않음 (WinAPI 명령어로 열람 가능)

레지스트리 하이브 파일 분석 (REGA 1.6.0.0 이용)

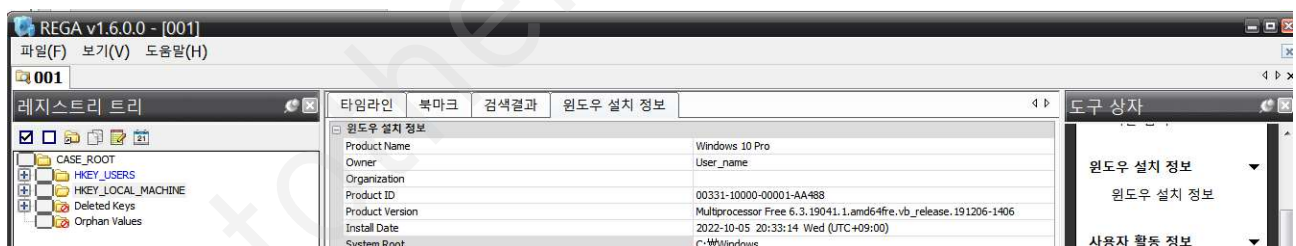
해당 시스템 내 Windows 깔려 있는 볼륨(파티션) 내 '%SystemRoot%\System32\config\' 하위 SYSTEM, SAM, SECURITY, SOFTWARE 추출,

'C:\Users\(\각 사용자 계정 폴더)\' 하위의 'NTUSER.DAT' 각각 추출함.

REGA 실행 후 '(UTC+09:00) 서울' 표준시간대 설정
추출된 레지스트리 파일 입력하여 분석 시작.

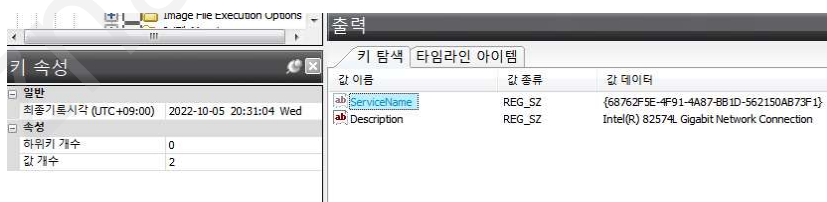


1. Windows 설치 정보 확인



2. 네트워크 카드(NIC) 정보 확인

1) 모델명 및 GUID 확인



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\2

모델명 및 GUID 확인을 위해 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\' 하위 검색

2) DHCP IP Address 확인

REGA v1.6.0.0 - [001]

파일(F) 보기(V) 도움말(H)

001

레지스트리 트리

타임라인 북마크 검색결과 윈도우 설치 정보

키 이름 설명 키 경로

출력

키 탐색 타임라인 아이템

값 이름	값 종류	값 데이터
EnableDHCP	REG_DWORD	00000001
Domain	REG_SZ	
NameServer	REG_SZ	
DhcpIPAddress	REG_SZ	192.168.91.128
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	192.168.91.254
Lease	REG_DWORD	00000708
LeaseObtainedTime	REG_DWORD	633EC1AD
T1	REG_DWORD	633EC531
T2	REG_DWORD	633EC7D4
LeaseTerminatesTime	REG_DWORD	633EC8B5
AddressType	REG_DWORD	00000000
IsServerNapAware	REG_DWORD	00000000
DhcpConnForceBroadcastFlag	REG_DWORD	00000000
DhcpDomain	REG_SZ	localdomain
DhcpNameServer	REG_SZ	192.168.91.2
DhcpDefaultGateway	REG_MULTI_SZ	192.168.91.2
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0
DhcpInterfaceOptions	REG_BINARY	FC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 89 03 ...
DhcpGatewayHardware	REG_BINARY	C0 A8 5B 02 06 00 00 00 50 56 FB D4 92
DhcpGatewayHardwareCount	REG_DWORD	00000001

키 속성

일반

최종기록시각 (UTC+09:00) 2022-10-06 20:53:17 Thu

속성

하위키 개수 0

값 개수 21

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpiip\Parameters\Interfaces\{504a2ddc-349a-11e1-8000-000000000000}

‘HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpiip\Parameters\Interfaces\(\해당 식별자:GUID)’ 하위 값(Dhcp IPAddress/SubnetMask/Server, DhcpNameServer) 검색하여 DHCP IP Address 및 부가 정보 확인.

3) MAC Address 확인

REGA v1.6.0.0 - [001]

파일(F) 보기(V) 도움말(H)

001

레지스트리 트리

타임라인 북마크 검색결과 윈도우 설치 정보

키 이름 설명 키 경로

출력

키 탐색 타임라인 아이템

값 이름	값 종류	값 데이터
IfType	REG_DWORD	00000006
MediaType	REG_DWORD	00000000
PhysicalMediaType	REG_DWORD	0000000E
IfAlias	REG_SZ	Ethernet0
NetLuidIndex	REG_DWORD	00008001
Characteristics	REG_DWORD	00000084
IfDescr	REG_SZ	Intel(R) 82574L Gigabit Network Connection
ProtocolList	REG_MULTI_SZ	RDMA\NDK Tcpiip MsLdp Tcpiip6 rpsndr RasPppoe Ndisuio II...
FilterList	REG_BINARY	DD DA 0B 43 B0 BA AB 41 A3 69 94 B6 7F A5 BE 0A 00 00...
CurrentAddress	REG_BINARY	00 0C 29 7F FB 2E
PermanentAddress	REG_BINARY	00 0C 29 7F FB 2E

키 속성

일반

최종기록시각 (UTC+09:00) 2022-10-05 20:31:04 Wed

속성

하위키 개수 0

값 개수 11

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\NetworkSetup2\Interfaces\{GUID}\Kernel\

‘HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\NetworkSetup2\Interfaces\{GUID}\Kernel\’ 키 내 MAC Address 확인

추가) 이벤트 로그 확인(무선 네트워크일 시)

‘/Windows/System32/winevt/Logs/Microsoft-Windows-Dhcp-Client%4Admin.evtx’ 추출하여 이벤트 뷰어에서 열기

이벤트 뷰어

파일(F) 동작(A) 보기(V) 도움말(H)

이벤트 뷰어 (로컬)

- > 사용자 지정 보기
- > Windows 로그
- > 응용 프로그램 및 서비스 로그
- > 저장된 로그
 - current_system_winevt
 - Microsoft-Windows-Dhcp-Client%4Admin

Microsoft-Windows-Dhcp-Client%4Admin 이벤트 수: 1

수준	날짜 및 시간	원본	이벤트 ...	작업 범...
정보	2022-09-15 오전 11:01:45	Dhcp-C...	50041	DNS 상...

이벤트 50041, Dhcp-Client

일반 자세히

☒ 간단히 보기(N) ☐ XML 보기(X)

- System
 - Provider
 - [Name] Microsoft-Windows-Dhcp-Client
 - [Guid] {15a7a4f8-0072-4eab-abad-f98a4d666aed}
 - EventID 50041
 - Version 0
 - Level 4
 - Task 6
 - Opcode 71
 - Keywords 0x4000000000000000
- TimeCreated
 - [SystemTime] 2022-09-15T02:01:45.6983599Z
 - EventRecordID 1
 - Correlation
- Execution
 - [ProcessID] 1596
 - [ThreadID] 1632
 - Channel Microsoft-Windows-Dhcp-Client/Admin
 - Computer WIN-DKFR0FCI3CU
- Security
 - [UserID] S-1-5-19

EventData

3. 유·무선 공유기 정보 확인

1) 네트워크카드(NIC) 정보 확인

The screenshot shows the Windows Registry Editor with the following path: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{18F78452-CEA3-4A68-A080-94D22440A5E5}`. The right pane displays the '키 탐색' (Key Explorer) and '타입라인 아이템' (Type List) for the selected profile.

값 이름	값 종류	값 데이터
ProfileName	REG_SZ	네트워크
Description	REG_SZ	네트워크
Managed	REG_DWORD	00000000
Category	REG_DWORD	00000000
DateCreated	REG_BINARY	E6 07 0A 00 03 00 05 00 14 00 20 00 14 00 D7 03
NameType	REG_DWORD	00000006
DateLastConnected	REG_BINARY	E6 07 0A 00 04 00 06 00 14 00 35 00 12 00 53 01

키 속성 (Key Properties):
 일반 (General): 최종 기록 시각 (UTC+09:00) 2022-10-06 20:53:18 Thu
 속성 (Attributes): 하위키 개수 0, 값 개수 7

시스템 설정 정보 (System Settings):
 Protected Storage
 실행 명령 (Run Command)
 검색 키워드 (Search Keywords)
 IE - 열려본 페이지 (IE - Opened Pages)
 원격 데스크톱 연결 (Remote Desktop Connection)
 네트워크 드라이브 연결 (Network Drive Connection)
 최근 실행 파일 (Recent Documents)
 ShellBag

‘HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\(\공유기의 GUID)\’의 하위 값들로 SSID(해당 네트워크 이름), 최초/최종 접속일시 정보 확인

2) MAC Address 확인

The screenshot shows the Windows Registry Editor with the following path: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\{010103000F0000F0080000000F0000F0747C}`. The right pane displays the '키 탐색' (Key Explorer) and '타입라인 아이템' (Type List) for the selected signature.

값 이름	값 종류	값 데이터
ProfileGuid	REG_SZ	{18F78452-CEA3-4A68-A080-94D22440A5E5}
Description	REG_SZ	네트워크
Source	REG_DWORD	00000008
DnsSuffix	REG_SZ	<없음>
FirstNetwork	REG_SZ	네트워크
DefaultGatewayMac	REG_BINARY	00 50 56 FB D4 92

키 속성 (Key Properties):
 일반 (General): 최종 기록 시각 (UTC+09:00) 2022-10-05 20:32:20 Wed
 속성 (Attributes): 하위키 개수 0, 값 개수 6

시스템 설정 정보 (System Settings):
 사용자 계정 정보 (User Account Information)
 Protected Storage
 실행 명령 (Run Command)
 검색 키워드 (Search Keywords)
 IE - 열려본 페이지 (IE - Opened Pages)
 원격 데스크톱 연결 (Remote Desktop Connection)
 네트워크 드라이브 연결 (Network Drive Connection)
 최근 실행 파일 (Recent Documents)
 ShellBag

‘HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\’ 하위 키(Managed 또는 Unmanaged) 선택하여 MAC Address 확인