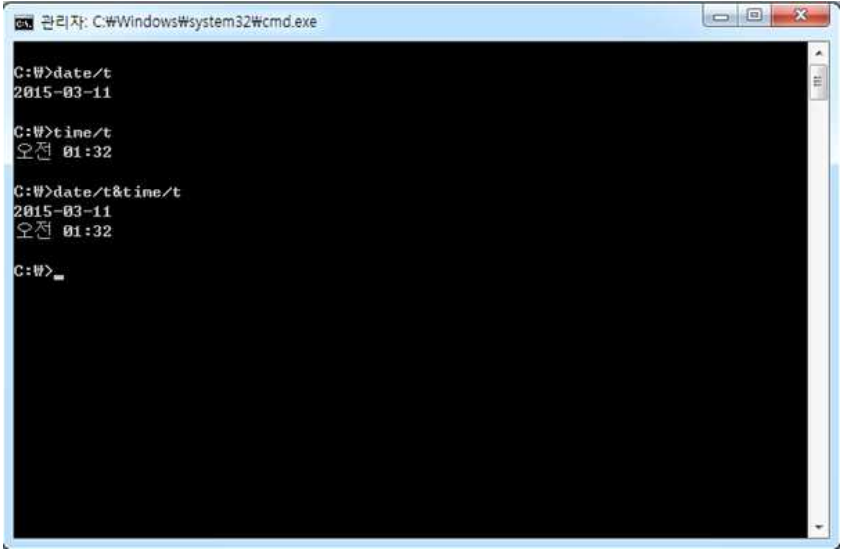


실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>현재 시스템의 날짜와 시간을 확인</p> <pre> c:\W>date/t c:\W>time/t c:\W>date/t&time/t </pre>		
실습 결과	 <p>The screenshot shows a Windows command prompt window titled '관리자: C:\Windows\system32\cmd.exe'. It displays the following commands and their outputs:</p> <pre> C:\W>date/t 2015-03-11 C:\W>time/t 오전 01:32 C:\W>date/t&time/t 2015-03-11 오전 01:32 C:\W> </pre>		
기 타	시스템 시간은 수정 가능하므로 Cell Phone과 비교		

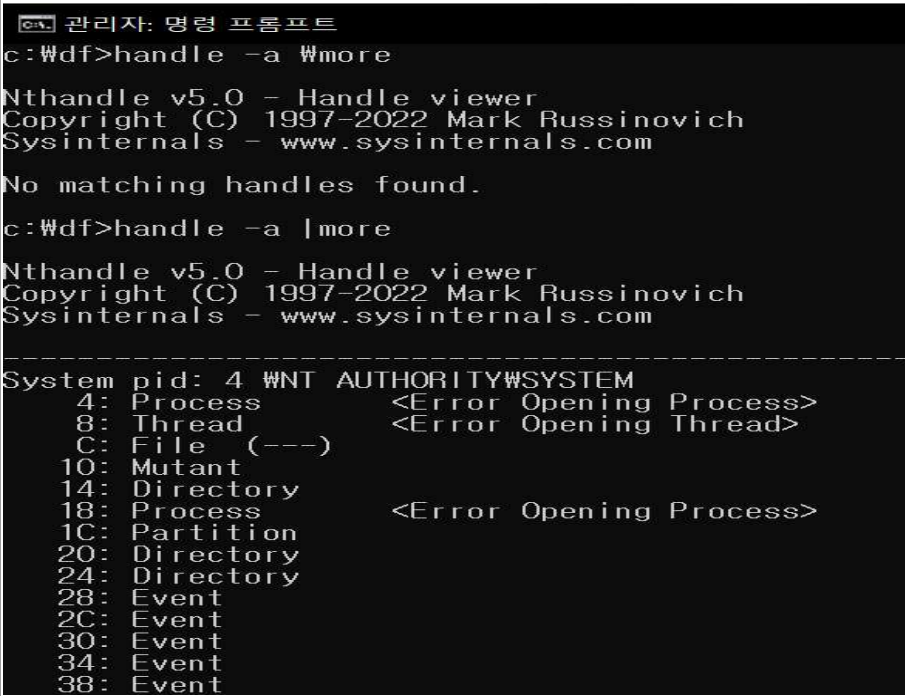
실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>netstat : 네트워크에서 열려 있는 포트 정보 등 조회</p> <p>C:\Users\Wjsb>netstat -nao</p>		
실습 결과	<pre> C:\Users\Wjsb>netstat -nao 활성 연결 프로토콜 로컬 주소 외부 주소 상태 PID TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1152 TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4 TCP 0.0.0.0:902 0.0.0.0:0 LISTENING 5488 TCP 0.0.0.0:912 0.0.0.0:0 LISTENING 5488 TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 9040 TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4 TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 920 TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 820 TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1632 TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 2072 TCP 0.0.0.0:49670 0.0.0.0:0 LISTENING 4188 TCP 0.0.0.0:49672 0.0.0.0:0 LISTENING 908 TCP 127.0.0.1:9528 0.0.0.0:0 LISTENING 4968 TCP 127.0.0.1:49698 127.0.0.1:49699 ESTABLISHED 1288 TCP 127.0.0.1:49699 127.0.0.1:49698 ESTABLISHED 1288 TCP 127.0.0.1:49700 127.0.0.1:49701 ESTABLISHED 2056 TCP 127.0.0.1:49701 127.0.0.1:49700 ESTABLISHED 2056 TCP 127.0.0.1:49703 127.0.0.1:49704 ESTABLISHED 5044 TCP 127.0.0.1:49704 127.0.0.1:49703 ESTABLISHED 5044 TCP 127.0.0.1:60195 127.0.0.1:5357 TIME_WAIT 0 TCP 127.0.0.1:60236 0.0.0.0:0 LISTENING 12780 TCP 192.168.111.1:139 0.0.0.0:0 LISTENING 4 </pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>네트워크 공유 폴더 정보</p> <p>C:\Users\Wjsb>net use</p>		
실습 결과			
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	프로세스 목록 조회 C:\Users\Wjsb>tasklist		
실습 결과	<pre> C:\Users\Wjsb>tasklist 이미지 이름 PID 세션 이름 세션# 메모리 사용 ----- System Idle Process 0 Services 0 8 K System 4 Services 0 148 K Registry 148 Services 0 33,596 K smss.exe 528 Services 0 1,236 K csrss.exe 724 Services 0 6,364 K wininit.exe 820 Services 0 7,576 K services.exe 908 Services 0 11,944 K lsass.exe 920 Services 0 21,636 K svchost.exe 728 Services 0 34,672 K fontdrvhost.exe 588 Services 0 5,016 K WUDFHost.exe 1088 Services 0 8,800 K svchost.exe 1152 Services 0 17,428 K svchost.exe 1200 Services 0 8,936 K WUDFHost.exe 1288 Services 0 19,128 K svchost.exe 1372 Services 0 9,688 K svchost.exe 1384 Services 0 8,792 K svchost.exe 1408 Services 0 11,640 K svchost.exe 1416 Services 0 11,792 K svchost.exe 1564 Services 0 10,800 K svchost.exe 1632 Services 0 23,868 K svchost.exe 1696 Services 0 10,568 K svchost.exe 1712 Services 0 12,248 K svchost.exe 1828 Services 0 7,856 K svchost.exe 1880 Services 0 8,432 K </pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	c:\wdf>tlist 실행 중인 프로세스와 관련 정보 실행 중인 프로세스 나열: 시스템에서 실행 중인 모든 프로세스와 프로세스 ID(PID)를 표시		
실습 결과			
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	c:\Wdf>pslist 실행 중인 프로세스의 리스트와 메모리, cpu 사용량 등 실행 특징출력		
실습 결과	<pre> c:\Wdf>pslist PsList v1.41 - Process information lister Copyright (C) 2000-2023 Mark Russinovich Sysinternals - www.sysinternals.com Process information for DESKTOP-BBOD1AQ: Name Pid Pri Thd Hnd Priv CPU Time Elapsed Time ----- Idle 0 0 12 0 60 1:36:32.062 3:11:52.583 System 4 8 278 4583 196 0:00:54.562 3:11:52.583 Registry 148 8 4 0 11404 0:00:03.156 3:11:55.315 smss 528 11 2 53 1088 0:00:00.109 3:11:52.581 csrss 724 13 13 74 2348 0:00:00.828 3:11:43.108 wininit 820 13 1 169 1708 0:00:00.031 3:11:42.858 services 908 9 6 827 6456 0:00:02.484 3:11:42.834 lsass 920 9 9 1442 8284 0:00:03.046 3:11:42.825 svchost 728 8 19 1625 13164 0:00:12.984 3:11:42.768 fontdrvhost 588 8 5 50 2108 0:00:00.015 3:11:42.764 WUDFHost 1088 8 7 301 4344 0:00:00.015 3:11:42.756 svchost 1152 8 12 1417 9804 0:00:08.109 3:11:42.719 svchost 1200 8 5 332 2900 0:00:00.437 3:11:42.705 WUDFHost 1288 13 20 447 9312 0:00:10.218 3:11:42.665 svchost 1372 8 7 158 5540 0:00:00.718 3:11:42.635 svchost 1384 8 3 200 1968 0:00:00.046 3:11:42.634 svchost 1408 8 2 177 1832 0:00:00.062 3:11:42.633 svchost 1416 8 7 270 2708 0:00:00.062 3:11:42.632 </pre>		
기 타	-t : Tree 형식, -x 프로세스가 사용하는 메모리와 스레드		

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>커널이 관리하는 오브젝트들에 할당되는 유일한 값 핸들이 실제로 가르키고 있는 오브젝트는 레지스트리에 기록 c:\Wdf>handle -a more</p>		
실습 결과	 <pre> 관리자: 명령 프롬프트 c:\Wdf>handle -a Wmore Nthandle v5.0 - Handle viewer Copyright (C) 1997-2022 Mark Russinovich Sysinternals - www.sysinternals.com No matching handles found. c:\Wdf>handle -a more Nthandle v5.0 - Handle viewer Copyright (C) 1997-2022 Mark Russinovich Sysinternals - www.sysinternals.com ----- System pid: 4 WNT AUTHORITY\SYSTEM 4: Process <Error Opening Process> 8: Thread <Error Opening Thread> C: File (---) 10: Mutant 14: Directory 18: Process <Error Opening Process> 1C: Partition 20: Directory 24: Directory 28: Event 2C: Event 30: Event 34: Event 38: Event </pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	dll 파일 정보 c:\>listdlls		
실습 결과	<pre> c:\>listdlls Listdlls v3.2 - Listdlls Copyright (C) 1997-2016 Mark Russinovich Sysinternals Error opening System(4): 액세스가 거부되었습니다. Error opening Registry(148): 액세스가 거부되었습니다. Error opening smss.exe(528): 액세스가 거부되었습니다. Error opening csrss.exe(724): 액세스가 거부되었습니다. Error opening wininit.exe(820): 액세스가 거부되었습니다. Error opening services.exe(908): 액세스가 거부되었습니다. ----- lsass.exe pid: 920 Command line: C:\WINDOWS\system32\lsass.exe Base Size Path 0x00000000537e0000 0x12000 C:\WINDOWS\system32\lsass.exe </pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	원격에서 로그인 한 사용자 정보 c:\wdf>net session		
실습 결과			
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	로컬 사용자와 원격 사용자 정보 모두 조회 c:\>psloggedon		
실습 결과	<pre>c:\>psloggedon PsLoggedon v1.35 - See who's logged on Copyright (C) 2000-2016 Mark Russinovich Sysinternals - www.sysinternals.com Users logged on locally: 2024-12-17 ?? 2:16:26 DESKTOP-BBOD1AQWjsb No one is logged on via resource shares.</pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	시스템에서 현재 활성화된 로그인 세션에 대한 정보를 표시 c:\wdf>logonsessioins		
실습 결과	<pre>c:\wdf>logonsessioins 'logonsessioins'은(는) 내부 또는 외부 명령, 실행할 수 있는 프로그램, 또는 배치 파일이 아닙니다.</pre>		
기 타	옵션 /p : 사용자가 사용하고 있는 프로세스 정보 제공		

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>파일이 가진 핸들 수집</p> <p>c:\wdf>net file</p>		
실습 결과			
기 타			

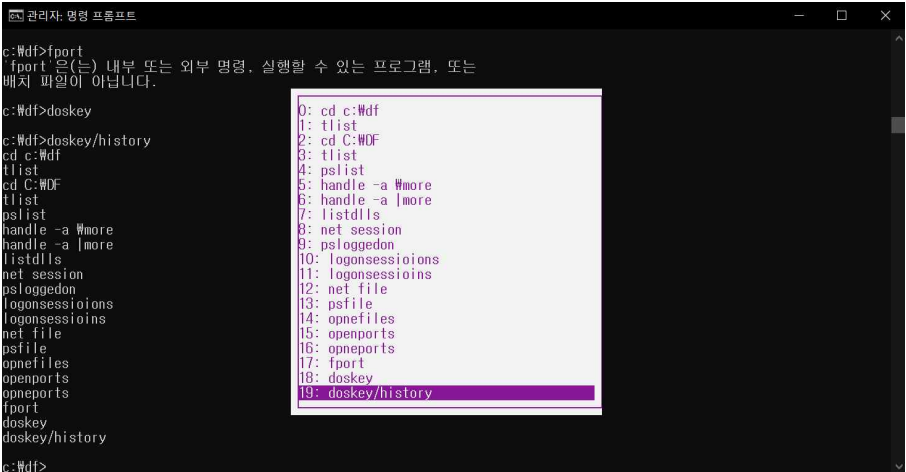
실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	원격 시스템에서 열려 있는 파일을 나열하고 해당 파일을 닫을 수 있는 기능 c:\>psfile		
실습 결과	<pre> c:\>psfile PsFile v1.04 - Lists files and directories opened remotely Copyright (C) 2001-2023 Mark Russinovich Sysinternals No files opened remotely on DESKTOP-BBOD1AQ. </pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	원격으로 열린 파일 확인 공유 파일이 없는 경우 " 공유된 열린 파일이 없습니다"		
실습 결과	<pre>c:\>df>opnefiles 'opnefiles'은(는) 내부 또는 외부 명령, 실행할 수 있는 프로그램, 또는 배치 파일이 아닙니다.</pre>		
기 타			

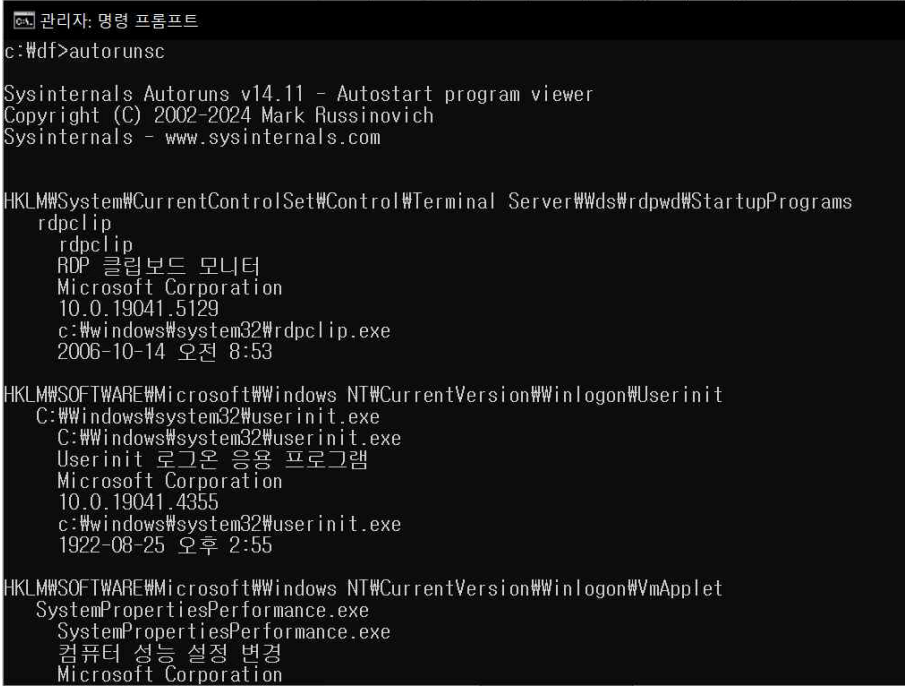
실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>시스템 프로세스와 함께 모든 열린 tcp와 udp 포트 정보 출력</p> <p>c:\>opneports</p>		
실습 결과	<p>c:\>opneports</p> <p>'opneports'은(는) 내부 또는 외부 명령, 실행할 수 있는 프로그램, 또는 배치 파일이 아닙니다.</p>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>해당 포트에 대한 맵핑 프로그램 정보</p> <p>c:\wdf>fport</p>		
실습 결과	<p>c:\wdf>fport</p> <p>'fport'은(는) 내부 또는 외부 명령, 실행할 수 있는 프로그램, 또는 배치 파일이 아닙니다.</p>		
기 타	<p>옵션 /p(포트로 정렬), /ap(응용프로그램 디렉터리로 정렬), /a응용프로그램, /i(프로세스 ID로 정렬)</p>		

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	커맨드 히스토리 c:\Wdf>doskey/history		
실습 결과	<pre> c:\Wdf>doskey/history cd c:\Wdf tlist cd C:\WDF tlist pslist handle -a Wmore handle -a I more listdlls net session psloggedon logonsessionioins logonsessionioins net file psfile opnefiles openports opneports fport doskey doskey/history </pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	명령 프롬프트에서 사용한 명령어 확인 Function Key : F7		
실습 결과			
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	악성 프로그램이 서비스에 등록 및 실행 여부 확인 c:\Wdf>psservice		
실습 결과	<pre>c:\Wdf>psservice PsService v2.26 - Service information and configuration utility Copyright (C) 2001-2023 Mark Russinovich Sysinternals - www.sysinternals.com SERVICE_NAME: AJRouter DISPLAY_NAME: AllJoyn Router Service 로컬 AllJoyn 클라이언트에 대해 AllJoyn 메시지를 라우팅합니다. 이 서비스를 중지하면 자체에 변들된 라우터가 없는 AllJoyn 클라이언트는 실행할 수 없습니다. TYPE : 20 WIN32_SHARE_PROCESS STATE : 1 STOPPED (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN) WIN32_EXIT_CODE : 1077 (0x435) SERVICE_EXIT_CODE : 0 (0x0) CHECKPOINT : 0x0 WAIT_HINT : 0 ms SERVICE_NAME: ALG DISPLAY_NAME: Application Layer Gateway Service 인터넷 연결 공유를 위한 타사 프로토콜 플러그 인을 지원합니다. TYPE : 10 WIN32_OWN_PROCESS STATE : 1 STOPPED (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN) WIN32_EXIT_CODE : 1077 (0x435) SERVICE_EXIT_CODE : 0 (0x0) CHECKPOINT : 0x0 WAIT_HINT : 0 ms</pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	시작 프로그램 목록에 등록된 서비스 확인 경로, 날짜, 프로그램 명 등을 나타냄 c:\>autorunsc		
실습 결과			
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>네트워크 연결상태 정보</p> <p>c:\wdf>netstat</p>		
실습 결과	<pre> c:\wdf>netstat 활성 연결 프로토콜 로컬 주소 외부 주소 상태 TCP 127.0.0.1:49698 DESKTOP-BB0D1AQ:49699 ESTABLISHED TCP 127.0.0.1:49699 DESKTOP-BB0D1AQ:49698 ESTABLISHED TCP 127.0.0.1:49700 DESKTOP-BB0D1AQ:49701 ESTABLISHED TCP 127.0.0.1:49701 DESKTOP-BB0D1AQ:49700 ESTABLISHED TCP 127.0.0.1:49703 DESKTOP-BB0D1AQ:49704 ESTABLISHED TCP 127.0.0.1:49704 DESKTOP-BB0D1AQ:49703 ESTABLISHED TCP 192.168.219.103:49411 20.198.119.143:https ESTABLISHED TCP 192.168.219.103:60187 20.198.119.143:https ESTABLISHED TCP 192.168.219.103:60241 208.103.161.1:https ESTABLISHED TCP 192.168.219.103:60255 208.103.161.1:https ESTABLISHED TCP 192.168.219.103:60353 121.254.136.178:https CLOSE_WAIT TCP 192.168.219.103:60358 121.254.136.177:https CLOSE_WAIT TCP 192.168.219.103:60368 192.168.219.21:8009 ESTABLISHED TCP 192.168.219.103:60398 tp-in-f188:5228 ESTABLISHED TCP 192.168.219.103:60406 172.64.155.209:https ESTABLISHED TCP 192.168.219.103:60407 172.64.155.209:https ESTABLISHED TCP 192.168.219.103:60411 1:https ESTABLISHED TCP 192.168.219.103:60424 20.42.73.31:https TIME_WAIT TCP 192.168.219.103:60425 20.247.160.101:https TIME_WAIT TCP 192.168.219.103:60426 134:https ESTABLISHED </pre>		
기 타	<p>-a (모든 연결), -n (어드레스와 포트번호) , -o(pid), -p(연결된 포트).-r (라우팅 테이블)</p>		

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>네트워크 인터페이스 정보</p> <p>c:\wdf>ipconfig /all</p>		
실습 결과	<pre> c:\wdf>ipconfig /all Windows IP 구성 호스트 이름 : DESKTOP-BB0D1AQ 주 DNS 접미사 : 노드 유형 : 혼성 IP 라우팅 사용 : 아니요 WINS 프록시 사용 : 아니요 무선 LAN 어댑터 로컬 영역 연결* 9: 미디어 상태 : 미디어 연결 끊김 연결별 DNS 접미사 : 설명 : Microsoft Wi-Fi Direct Virtual Adapter 물리적 주소 : D4-E9-8A-B8-0C-28 DHCP 사용 : 예 자동 구성 사용 : 예 무선 LAN 어댑터 로컬 영역 연결* 10: 미디어 상태 : 미디어 연결 끊김 연결별 DNS 접미사 : 설명 : Microsoft Wi-Fi Direct Virtual Adapter #2 물리적 주소 : D6-E9-8A-B8-0C-27 DHCP 사용 : 아니요 자동 구성 사용 : 예 </pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	<p>네트워크 인터페이스가 **Promiscuous Mode(무차별 모드)**로 작동하고 있는지 여부를 감지하는 데 사용</p> <p>c:\>promiscdetect</p>		
실습 결과	<pre>c:\>promiscdetect 'promiscdetect'은(는) 내부 또는 외부 명령, 실행할 수 있는 프로그램, 또는 배치 파일이 아닙니다.</pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	작업 스케줄러 c:\wdf>schtasks		
실습 결과	<pre>c:\wdf>schtasks 폴더: \ 작업 이름 다음 실행 시간 상태 ===== LGAppCount N/A 준비 LGPCCareWin32 N/A 실행 중 LGUpdateRecovery N/A 준비 MicrosoftEdgeUpdateTaskMachineCore[F2ED8 2024-12-17 오전 9:46:3 준비 MicrosoftEdgeUpdateTaskMachineUA{306BC7B 2024-12-17 오전 3:16:3 준비 MicrosoftEdgeUpdateTaskUserS-1-5-21-3876 2024-12-17 오전 9:47:1 준비 MicrosoftEdgeUpdateTaskUserS-1-5-21-3876 2024-12-17 오전 3:17:1 준비 npcapwatchdog N/A 준비 OneDrive Reporting Task-S-1-5-21-3876585 2024-12-17 오후 10:03: 준비 OneDrive Standalone Update Task-S-1-5-21 2024-12-17 오후 9:55:3 준비 Run LG Live Wallpaper N/A 실행 중 ZoomUpdateTaskUser-S-1-5-21-3876585285-3 2024-12-17 오전 8:09:0 준비 폴더: \GoogleSystem 작업 이름 다음 실행 시간 상태 ===== 정보:사용자의 액세스 수준에서 현재 사용할 수 있는 작업이 없습니다. 폴더: \GoogleSystem\GoogleUpdater 작업 이름 다음 실행 시간 상태 ===== GoogleUpdaterTaskSystem132.0.6833.0{757D 2024-12-17 오전 3:17:3 준비</pre>		
기 타			

실습분류 항목	Live Response	분류번호	L-01
세부점검 항목	시스템 시간	대상	Windows 7
실습 방법	Windows - cmd		
실습 내용	netbios 정보 c:\>netstat -c		
실습 결과	<pre> c:\>netstat -c 프로토콜 통계와 현재 TCP/IP 네트워크 연결을 표시합니다. NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval] -a 모든 연결 및 수신 대기 포트를 표시합니다. -b 각 연결 또는 수신 대기 포트 생성과 관련된 실행 파일을 표시합니다. 잘 알려진 실행 파일이 여러 독립 구성 요소를 호스팅할 경우 연결 또는 수신 대기 포트 생성과 관련된 구성 요소의 시퀀스가 표시됩니다. 이러한 경우에는 실행 파일 이름이 아래 [] 안에 표시되고 위에는 TCP/IP에 도달할 때까지 호출된 구성 요소가 표시됩니다. 이 옵션은 시간이 오래 걸릴 수 있으며 사용 권한이 없으면 실패합니다. -e 이더넷 통계를 표시합니다. 이 옵션은 -s 옵션과 함께 사용할 수 있습니다. -f 외부 주소의 FQDN(정규화된 도메인 이름)을 표시합니다. -n 주소 및 포트 번호를 숫자 형식으로 표시합니다. -o 각 연결의 소유자 프로세스 ID를 표시합니다. -p proto proto로 지정한 프로토콜의 연결을 표시합니다. proto는 TCP, UDP, TCPv6 또는 UDPv6 중 하나입니다. -s 옵션과 함께 사용하여 프로토콜별 통계를 표시할 경우 proto는 IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP 또는 UDPv6 중 하나입니다. -q 모든 연결, 수신 대기 포트 및 바인딩된 비수신 대기 TCP 포트를 표시합니다. 바인딩된 비수신 대기 포트는 활성 연결과 연결되거나 연결되지 않을 수도 있습니다. -r 라우팅 테이블을 표시합니다. </pre>		
기 타			

