※ 윈도우 원격데스크톱 접속로그 확인

1. 윈도우키(**●)+R** → "eventvwr" 입력 후 엔터

📨 실행	×					
	프로그램, 폴더, 문서 또는 인터넷 주소를 입력하십시오.					
열기(<u>O</u>):	veentvwr ☞ 이 작업은 관리자 권한으로 실행됩니다.					
	확인 취소 찾아보기(B)					

2. "응용 프로그램 및 서비스 로그" -> "Microsoft" -> "Windows" -> "TerminalServices-LocalSessionManager" -> "Operational"에서 접속 로그 확인

파일(F) 동작(A) 보기(V) 도움말(H)								
+	■ PowerShell Operational 이벤트 수: 1,731 Operational 이벤트 →: 1,731 Operational							
+	E 🧮 PrimaryNetworkIcon			나파 민 시가	위보			
+	E PrintService	교전보		2018-01-24 오늘 3:57:59	TerminalServices-			
+	E 🔜 HeadyBoost			2018-01-24 오늘 3:53:53	TerminalServices-			
+	B Booguory	제 정보		2018-01-24 오늘 3:53:29	TerminalServices-			
±	a 🦰 Beliabilitu-Analusis-Engine	전보		2018-01-24 오흐 3:53:09	TerminalServices-			
	BemoteAnn and Deskton Conr	전보		2018-01-23 오전 8:53:43	TerminalServices-			
Ŧ	RemoteAssistance	이정보		2018-01-22 오호 7:31:48	TerminalServices-			
+	🛛 🧰 RemoteDesktopServices-Rdp(전보		2018-01-22 오호 7:28:56	TerminalServices-			
+	🛛 🧰 RemoteDesktopServices-Rem	1						
+	🗉 🚞 Resource-Exhaustion-Detecto		and in all Carolines I a coll Caroline M					
+	🗉 🚞 Resource-Exhaustion-Resolv	이벤트 24, 1	erm inal Services-Local Sessioniv	anager	~			
+	🛛 🚞 Resource-Leak-Diagnostic 👘	일반 지						
+	🗉 🚞 RestartManager				1			
+	Security-Audit-Configuration-Configuratio							
+	E Security-IdentityListener	원격 네스	=크·통 서비스: 세선 연결 끊김: -					
±	E Service Reporting API							
+	B StickuNotoc	사용자: 니	JSE <mark>L</mark> -KO₩User					
		<u>세션 ID:</u>	1					
	TerminalServices-ClientActive	원본 네트	워크 주소: 143.248	- 좌즉 IP는 '원격연결'을	을 시도한 IP로, 이 IP가 해			
(H)	TerminalServices-ClientUSBD			당시간대에 보인이 사	용하 IP가 아닌경우 이는			
	🛛 🧰 TerminalServices-LocalSessi			케리카 이거에거요 나				
_	🔁 Admin			얘겨가 원격연결을 시	노안 은식이다.			
	Operational							
+	🗉 📫 TerminalServices-PnPDevices	로그 이름	(M): Microsoft-Wine	dows-TerminalServices-LocalSes	sionManager/Operational			
+	🗉 🚞 TerminalServices-RemoteCor		Torreito d'Orre de					
+	🗉 🚞 TerminalServices-ServerUSB[원론(S):	TerminalServic	es-LocalSessi 도그된 날짜(D):	2018-01-22 모후 7:31:48			
+	E 🛄 TZUtil	이벤트 ID	(E): 24	작업 범주(Y):	없음			
+			저비	71 91 E (K)-				
+	UAC-File Virtualization		0×	×1=(v).				
E E		사용자(U)	SYSTEM	컴퓨터(R):				
±		Opcode(C)): 정보					
	a 🦳 WeblO	*7.74		· • •				
(+)	🗉 🧰 WER-Diagnostics	우가 정보	(1). <u>이벤트 토그 토</u>	<u>52</u>				
	MEP	- I						

▶ 위의 경우로 확인한 결과, 의심스런 흔적이 발견되는 경우, <u>kaistcert@kaist.ac.kr</u> 또는 T. 2413로 문의하시기 바 랍니다.