105 – Who leaked the secret

Team Information

Team Name: ISEGYE_IDOL

Team Member: Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address: dfc-isegyeidol@googlegroups.com

Instructions

Description There was an incident where confidential documents were leaked. As a result of the investigation, it was confirmed that the leaked documents were scanned through one of the three suspects (A, B, C). In order to identify the leaker, forensic investigators obtained some of the leaked images (Secret01~02) and images scanned from the scanners of suspects A, B, and C (A01~A02, B01~B02, C01~C02).

Target	Hash (MD5)
Images.zip	260a8418dc390bd0f47621b8f58e27fc

Questions

- Identify which of the scanners A, B, or C scanned the leaked file, and provide objective evidence.

Teams must:

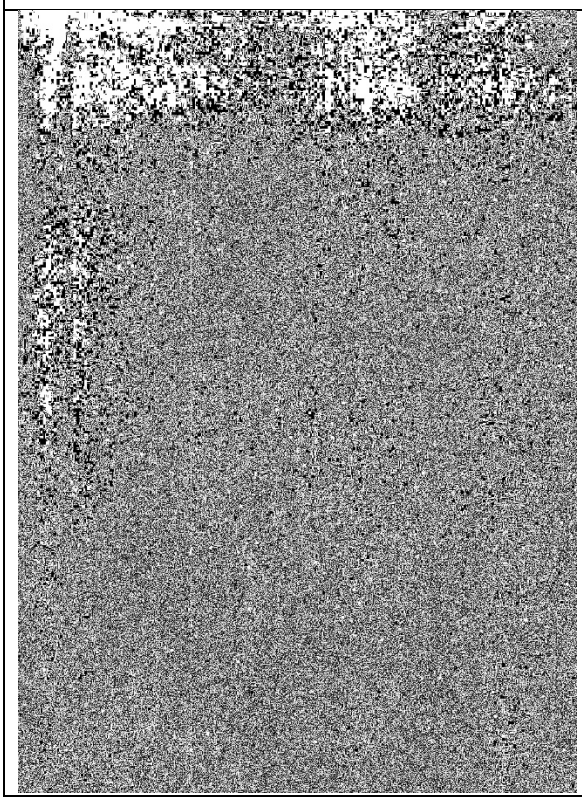
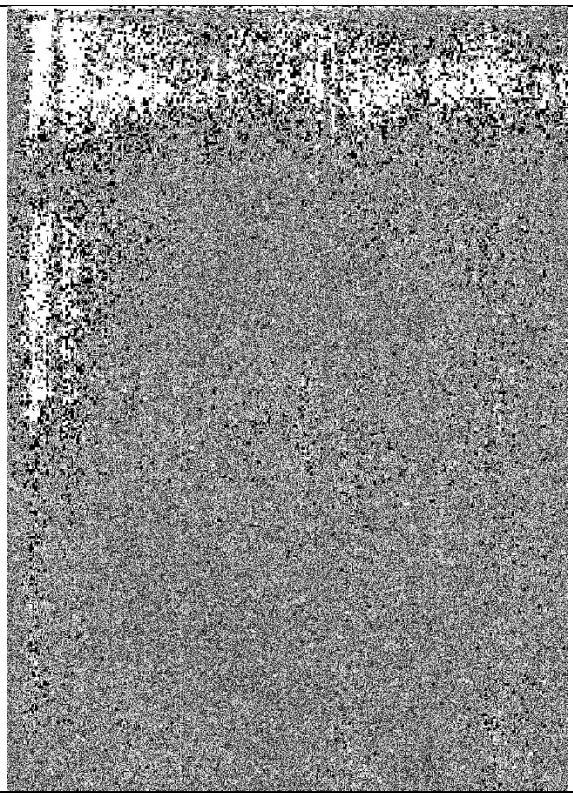
- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

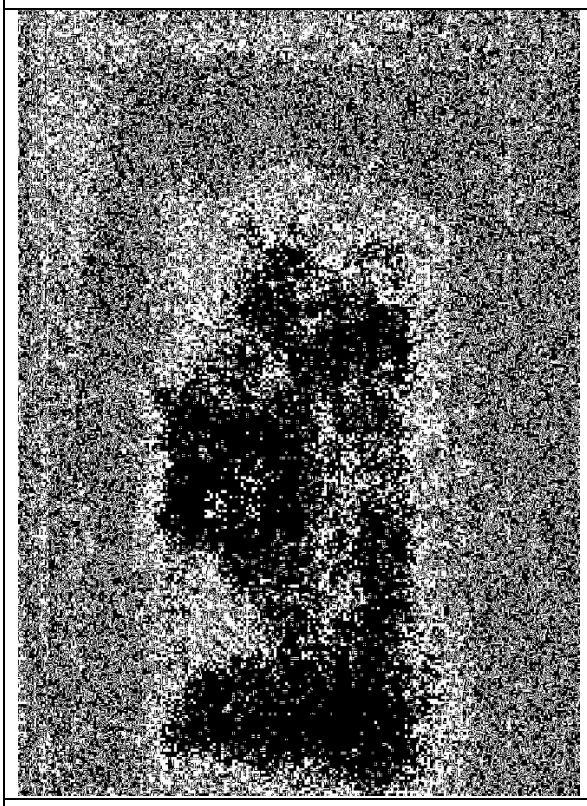
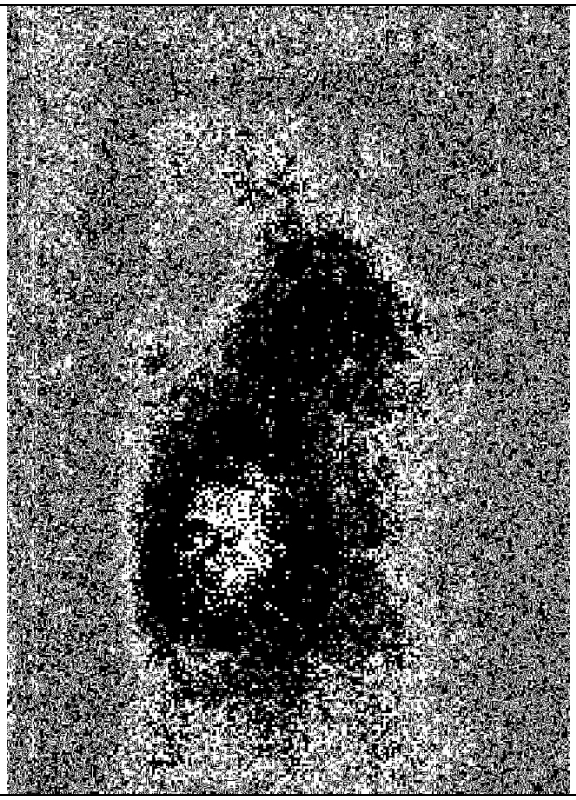
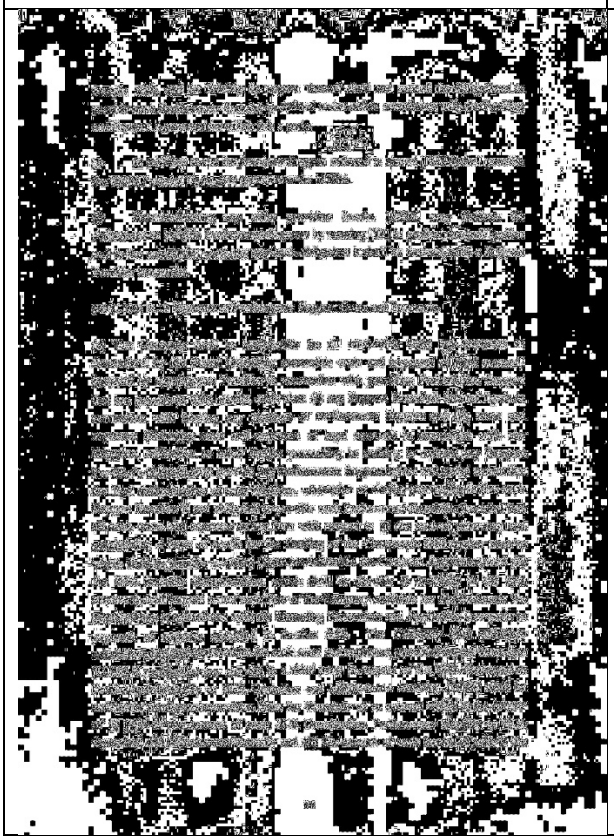
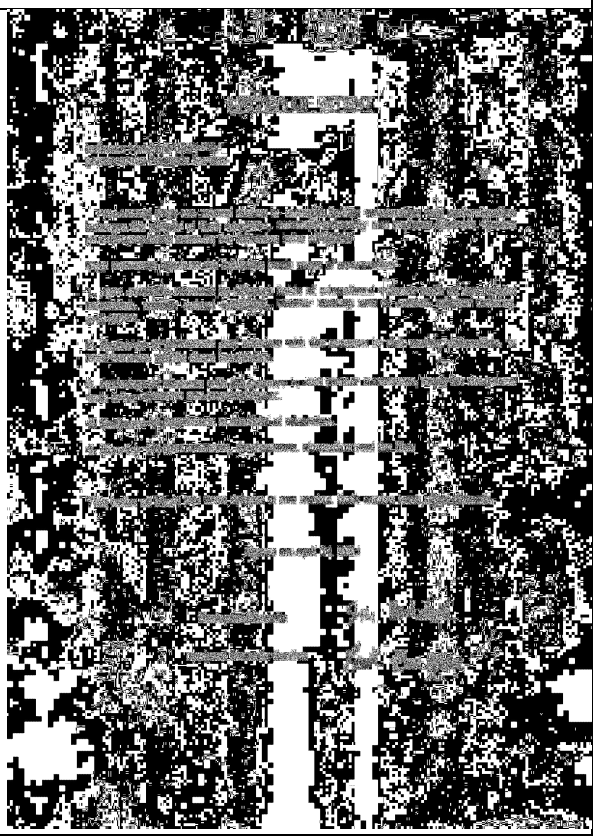
Tools used:

Name:	Stegsolve.jar	Publisher:	Caesum
Version:	1.3		
URL:	http://www.caesum.com/handbook/Stegsolve.jar		

Step-by-step methodology:

아래는 Stegsolve.jar를 사용하여 주어진 모든 이미지의 red plane 1의 결과 이미지이다.

A01	A02
	
B01	**B02**
	

C01	C02
	
Secret01	**Secret02**
	

각 스캐너 별로 고유한 패턴이 나타나는 것을 확인할 수 있다.

A01~02는 중앙에 두꺼운 하얀색 세로줄, B01~02는 상단에 얇은 하얀색 가로줄, C01~02는 중앙에 뭉친 검은색 영역이 특징이다. Secret에서 나타난 특징은 중앙에 두꺼운 하얀색 세로줄이므로 Secret01~02를 스캔한 용의자는 A라고 할 수 있다.