**Background:**

Alva & Drexel (A&D)是一家英国跨国集团，专门从事许多不同领域的业务，包括风力涡轮机。**A&D公司已经暂停了其一名软件工程师的工作，同时对该人为个人利益而泄露商业秘密的问题进行调查。**这些商业秘密包括与风力涡轮机的有效管理有关的**算法和数学模型**。

A&D代表称，该前雇员利用反鉴别技术渗出了重要的商业秘密，目的是为了。(1) 公开发布一些信息，(2) 将一些信息出售给其他实体，以及(3) 开始自己的竞争业务。

A&D代表提出这些主张的**依据是**，该人在几个月内通过可移动媒体在工作站和他们自己的个人设备之间传输了**超过20,000张图像**。A&D代表还截获了一些不寻常的电子邮件，这些电子邮件含有发送到该员工个人电子邮件账户的**图像**。

该组织认为，该员工利用可移动媒体和信息服务的组合，通过位图图像将商业秘密渗入到组织的外围。该员工表示，他们没有为个人利益渗入任何数据。

代表A&D的Rossum & Hamilton（R&H）律师事务所担心他们没有足够有力的证据来证明该软件工程师已经或将以A&D代表所建议的方式渗出数据。R&H不确定在这种特定情况下关于源代码、知识产权的法律论据，以及该雇员如何以该组织建议的方式获利

**Task:**

**任务是研究针对取证分析的对策，并通过报告和演示将其传达给非技术受众。**

该报告将用于确定团队的成绩。团队成员需要同意一份单页A4纸的工作量记录，并将其作为附录与报告一起列入。此外，团队成员需要通过分配100分来完成自己对队友的个人评估。如果个人不提交个人评估，则假定贡献相同。个人贡献评估是由每个团队成员在最终报告中单独提交的。每个团队成员的贡献评估将被用来作为个人练习成绩的依据。

**Non-programming Route:**

选择这条路线的团队需要制作一份**6页的报告**。

该路线的预期报告包括:

封面概述了团队的名称、成员、学生人数和字数。

认识问题，概述反取证学及其在特定背景下的挑战（1页）。

着重于反取证的四个关键领域（如数据隐藏、人工制品擦除、线索混淆等）的文献调查，并将其巩固在给定的环境中（3页）。

论证前软件工程师是否真的会以这种方式从组织中渗出数据（1页）。

论证该组织所寻求的案例是否可行，即具体而言，软件工程师利用公司工作站渗出商业秘密以谋取私利（提示：考虑外部环境，用相关证据加强论证）（1页）。

书目。

工作量报告详细说明成员的贡献（团队可简单说明所有成员贡献相同）。

**需要论证的是这名工程师通过可移动设备和电子邮件传输的图像包含商业机密内容的可能性，即通过这种方式去渗出数据是否可行。**

**还需要论证的是AD公司提出的该工程师渗透数据的可能性（通过位图图像），以及需要考虑外部环境的支持，需要强有力的证据。**

What Is Anti-Forensics?

Anti-forensics is a set of precautionary measures a user can perform in order to hide traces of his activity, making investigations on digital media more complicated and time-consuming, and potentially rendering evidence of illegal activities difficult or impossible to obtain. Detecting anti-forensic techniques in use is not always easy and not always possible, as destroying certain types of evidence may leave no traces anywhere in the system. However, since average users have little to average hi-tech knowledge, anti-forensic attempts they perform may be generally ineffective or obviously visible to the expert.

**Four key areas of anti-forensics:**

**1.Data hiding**

[Data hiding](https://en.wikipedia.org/wiki/Data_hiding) is the process of making data difficult to find while also keeping it accessible for future use. "[Obfuscation](https://en.wikipedia.org/wiki/Obfuscation) and [encryption](https://en.wikipedia.org/wiki/Encryption) of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."

Some of the more common forms of data hiding include encryption, [steganography](https://en.wikipedia.org/wiki/Steganography) and other various forms of hardware/software based data concealment. Each of the different data hiding methods makes digital forensic examinations difficult. When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.

**2.Artifact wiping**

The methods used in artifact wiping are tasked with permanently eliminating particular files or entire file systems. This can be accomplished through the use of a variety of methods that include disk cleaning utilities, file wiping utilities and disk degaussing/destruction techniques

**3.Trail obfuscation**

The purpose of trail obfuscation is to confuse, disorient, and divert the forensic examination process. Trail obfuscation covers a variety of techniques and tools that include "log cleaners, [spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing), [misinformation](https://en.wikipedia.org/wiki/Misinformation), backbone hopping, zombied accounts, trojan commands."

One of the more widely known trail obfuscation tools is Timestomp (part of the [Metasploit Framework](https://en.wikipedia.org/wiki/Metasploit_Framework)). Timestomp gives the user the ability to modify file [metadata](https://en.wikipedia.org/wiki/Metadata) pertaining to access, creation and modification times/dates. By using programs such as Timestomp, a user can render any number of files useless in a legal setting by directly calling into question the files' credibility.

Another well known trail-obfuscation program is Transmogrify (also part of the Metasploit Framework). In most file types the header of the file contains identifying information. A (.jpg) would have header information that identifies it as a ([.jpg](https://en.wikipedia.org/wiki/.jpg)), a ([.doc](https://en.wikipedia.org/wiki/.doc)) would have information that identifies it as (.doc) and so on. Transmogrify allows the user to change the header information of a file, so a (.jpg) header could be changed to a (.doc) header. If a forensic examination program or [operating system](https://en.wikipedia.org/wiki/Operating_system) were to conduct a search for images on a machine, it would simply see a (.doc) file and skip over it

**4.Attacks against computer forensics**

In the past anti-forensic tools have focused on attacking the forensic process by destroying data, hiding data, or altering data usage information. Anti-forensics has recently moved into a new realm where tools and techniques are focused on attacking forensic tools that perform the examinations. These new anti-forensic methods have benefited from a number of factors to include well documented forensic examination procedures, widely known forensic tool vulnerabilities, and digital forensic examiners' heavy reliance on their tools.

During a typical forensic examination, the examiner would create an image of the computer's disks. This keeps the original computer (evidence) from being tainted by forensic tools. [Hashes](https://en.wikipedia.org/wiki/Cryptographic_hash_function) are created by the forensic examination software to verify the [integrity](https://en.wikipedia.org/wiki/Data_integrity) of the image. One of the recent anti-tool techniques targets the integrity of the hash that is created to verify the image. By affecting the integrity of the hash, any evidence that is collected during the subsequent investigation can be challenged

1. [**https://doi.org/10.1016/j.diin.2006.06.005**](https://doi.org/10.1016/j.diin.2006.06.005)
2. 10.4225/75/57ad39ee7ff25
3. [**https://doi.org/10.1109/ICASSP.2012.6288237**](https://doi.org/10.1109/ICASSP.2012.6288237)**(提到了一系列数学模型，可以研究一下)**
4. [**https://doi.org/10.1049/iet-ipr.2018.6587**](https://doi.org/10.1049/iet-ipr.2018.6587)**（关于数字图像的）**
5. [**https://doi-org.ezproxy.lib.gla.ac.uk/10.1109/MSP.2017.4251117**](https://doi-org.ezproxy.lib.gla.ac.uk/10.1109/MSP.2017.4251117)**（遇到的挑战）**