第 4 章 MD5散列值碰撞 实验报告

环境配置

```
>systeminfo
...
OS Name:     Microsoft Windows 10 家庭中文版
OS Version:  10.0.19045 N/A Build 19045
...
```

实验步骤及结果

首先使用 `fastcoll` 生产 md5 碰撞文件，接下来使用 `certutil` 验证文件 MD5 碰撞，并验证 SHA-1值不同。

```
.\fastcoll_v1.0.0.5.exe -p C:\Windows\System32\calc.exe -o 1.exe 2.exe
certutil -hashfile 1.exe MD5
certutil -hashfile 2.exe MD5
certutil -hashfile 1.exe SHA1
certutil -hashfile 2.exe SHA1
```

```
(base) C:\Users\joshu\cyber_security_experiments\md5>.\fastcoll_v1.0.0.5.exe -p C:\Windows\System32\calc.exe -o 1.exe 2.exe
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: '1.exe' and '2.exe'
Using prefixfile: 'C:\Windows\System32\calc.exe'
Using initial value: 99e9ef7febe0ef41607b8759bf7f34a1

Generating first block: ................
Generating second block: S11.....
Running time: 6.937 s
```

```
(base) C:\Users\joshu\cyber_security_experiments\md5>certutil -hashfile 1.exe MD5
MD5 的 1.exe 哈希:
9108602d7b31129da74d4f13b35664df
CertUtil: -hashfile 命令成功完成。

(base) C:\Users\joshu\cyber_security_experiments\md5>certutil -hashfile 2.exe MD5
MD5 的 2.exe 哈希:
9108602d7b31129da74d4f13b35664df
CertUtil: -hashfile 命令成功完成。

(base) C:\Users\joshu\cyber_security_experiments\md5>certutil -hashfile 1.exe SHA1
SHA1 的 1.exe 哈希:
54250fa7b5812e090b720c6645aba0a09e77d38e
CertUtil: -hashfile 命令成功完成。

(base) C:\Users\joshu\cyber_security_experiments\md5>certutil -hashfile 2.exe SHA1
SHA1 的 2.exe 哈希:
249387e0950131745f3c54676594b24905b1647f
CertUtil: -hashfile 命令成功完成。
```

这说明 `1.exe` 和 `2.exe` 是两个具有相同 MD5 值的不同文件。