Category: Forensics
Challenge: Contacts

Write-up:

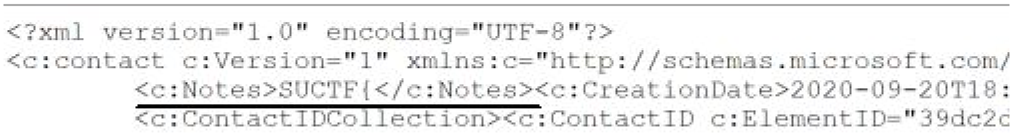
We are given a .ad1 file. When we research it, we can understand that it is a file type associated with Forensic Toolkit by Accessdata. It is an image file!

One can download many tools, but I will be using the FTK Imager, which Accessdata provides.

Since it is an image file, we need to open this evidence item as an Image File in the program. When we open it, we can see some folder and files under the root directory. Since the name of the challenge is "Contact", the first thing that is drawing attention is the folder named 'contacts'. After we open that folder, we can see some files.

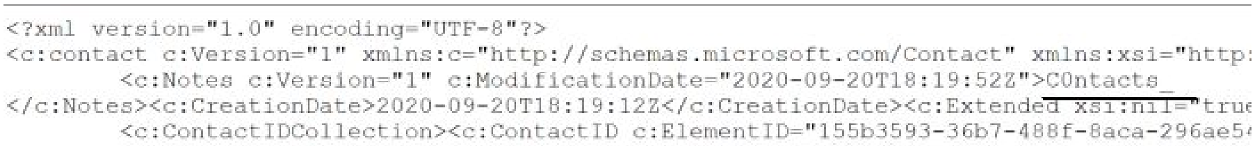
Short after looking at all those files in the folder "contacts", some files containing <c:Notes> </c:Notes> tag's that contain flags!

In the file dealer.contact:



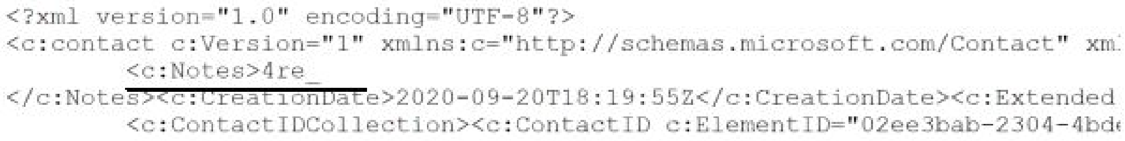
```
<?xml version="1.0" encoding="UTF-8"?>
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/
        <c:Notes>SUCTF{</c:Notes><c:CreationDate>2020-09-20T18:
        <c:ContactIDCollection><c:ContactID c:ElementID="39dc2c
```

In the file broker.contact:



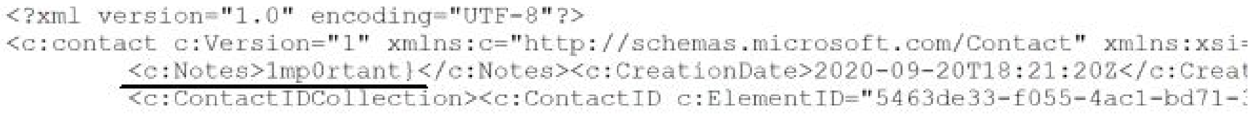
```
<?xml version="1.0" encoding="UTF-8"?>
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact" xmlns:xsi="http:
        <c:Notes c:Version="1" c:ModificationDate="2020-09-20T18:19:52Z">C0ntacts_
</c:Notes><c:CreationDate>2020-09-20T18:19:12Z</c:CreationDate><c:Extended xsi:nil="true
        <c:ContactIDCollection><c:ContactID c:ElementID="155b3593-36b7-488f-8aca-296ae5
```

In the file target.contact:



```
<?xml version="1.0" encoding="UTF-8"?>
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact" xm
        <c:Notes>4re_
</c:Notes><c:CreationDate>2020-09-20T18:19:55Z</c:CreationDate><c:Extended
        <c:ContactIDCollection><c:ContactID c:ElementID="02ee3bab-2304-4bd
```

In the file Money Giver.contact:



```
<?xml version="1.0" encoding="UTF-8"?>
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact" xmlns:xsi=
        <c:Notes>1mp0rtant}</c:Notes><c:CreationDate>2020-09-20T18:21:20Z</c:Creat
        <c:ContactIDCollection><c:ContactID c:ElementID="5463de33-f055-4ac1-bd71-
```

When we add all of these notes into the another, we can get the flag.
Flag is: SUCTF{C0ntacts_4re_1mp0rtant}