Lab 6: Update Sequence Number (USN) Journaling

What You Need for this lab

- Install Virtualbox : https://www.virtualbox.org/wiki/Downloads

- Install Kali 2021.4. : https://old.kali.org/kali-images/kali-2021.4/

  - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+

- https://www.dropbox.com/sh/3lyzpi7vyod0pfs/AADh2b3TnmMqWZHB1Uzv9_ma?dl=0
- https://ubaltmy.sharepoint.com/:f:/g/personal/id31ga53_ubalt_edu/EoJThlUPE85Hm7592HB5sjIBGo4Ht9drLxt9XnwDdnf3PA?e=4Okj4m
- https://github.com/jschicht/ExtractUsnJrnl
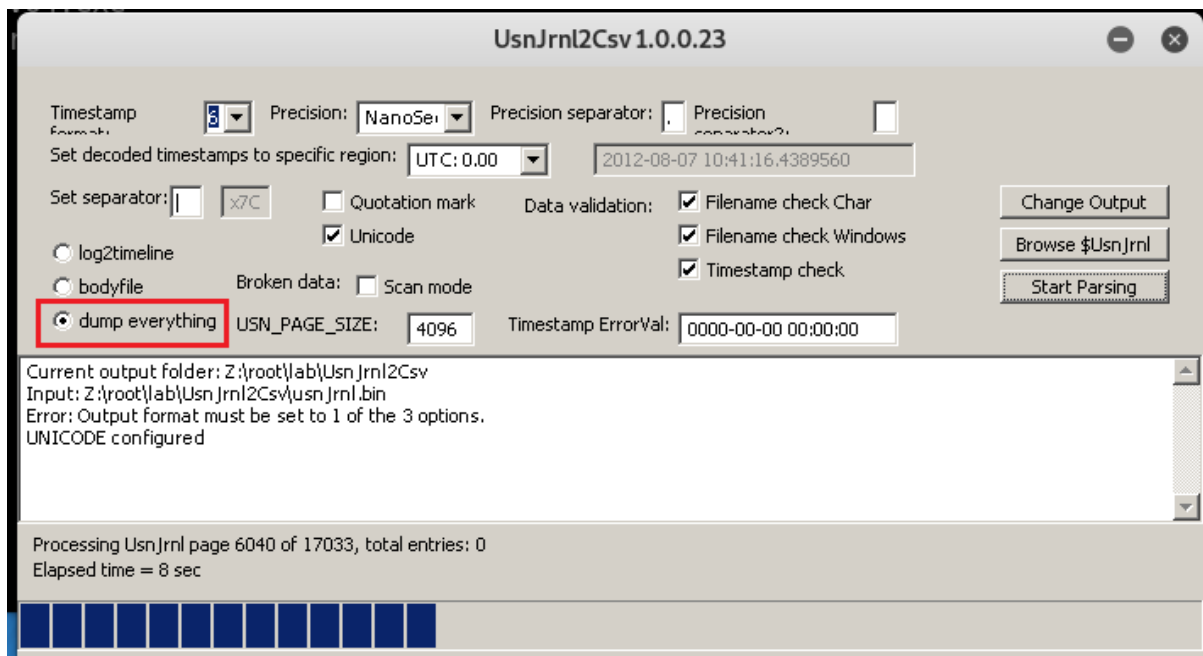
- Image .dd from Lab 5

Scenario 1

- Install *UsnJrnl2Csv* tool

- Run *UsnJrnl2.exe* to covert *UsnJrnl.bin* to .csv

- Set configuration: Browser to *usnJrnl.bin*

– Show the extracted USN journal file

– Only show "*RENAME_OLD*" information of any .jpg files

– Only show "RENAME_OLD" information of any .jpg files. Only show three columns, FileName, Timestamp, Reason

```
                                            /bin/bash 97x35
root@kali:~/lab/UsnJrnl2Csv#
root@kali:~/lab/UsnJrnl2Csv# awk '{print NR, $2, $4, $5}' FS='|' UsnJrnl_2020-11-28_12-15-14.csv
 | grep -E "\.jpg.*RENAME_OLD" --color
261131 Chrysanthemum.jpg 2015-03-24 20:11:42.8361742 RENAME_OLD_NAME
261139 Desert.jpg 2015-03-24 20:11:42.8517742 RENAME_OLD_NAME
261155 Hydrangeas.jpg 2015-03-24 20:11:42.8517742 RENAME_OLD_NAME
261171 Jellyfish.jpg 2015-03-24 20:11:42.8517742 RENAME_OLD_NAME
261179 Koala.jpg 2015-03-24 20:11:42.8517742 RENAME_OLD_NAME
261187 Lighthouse.jpg 2015-03-24 20:11:42.8517742 RENAME_OLD_NAME
261195 Penguins.jpg 2015-03-24 20:11:42.8517742 RENAME_OLD_NAME
261203 Tulips.jpg 2015-03-24 20:11:42.8517742 RENAME_OLD_NAME
299494 Chrysanthemum.jpg 2015-03-25 15:13:39.1698055 RENAME_OLD_NAME
299536 Desert.jpg 2015-03-25 15:13:39.4350055 RENAME_OLD_NAME
299578 Hydrangeas.jpg 2015-03-25 15:13:39.5442055 RENAME_OLD_NAME
299665 Jellyfish.jpg 2015-03-25 15:13:48.8730055 RENAME_OLD_NAME
299707 Koala.jpg 2015-03-25 15:13:49.0602055 RENAME_OLD_NAME
299749 Lighthouse.jpg 2015-03-25 15:13:49.2162055 RENAME_OLD_NAME
299791 Penguins.jpg 2015-03-25 15:13:49.3566055 RENAME_OLD_NAME
299833 Tulips.jpg 2015-03-25 15:13:49.4658055 RENAME_OLD_NAME
root@kali:~/lab/UsnJrnl2Csv#
```

– Show what has happened around a specific time with the same MFT reference #

```
  # grep  "2015-03-24 20:11.*|74620|"  UsnJrnl_2021-10-12_12-36-58.csv
0x03D6BCA0|Chrysanthemum.jpg|64404640|2015-03-24 20:11:42.8361742|RENAME_OLD_NAME|74620|285|21921|3|archiv
e|2|0|0x00000000|0
0x03D6BD00|$RKXD1U3.jpg|64404736|2015-03-24 20:11:42.8361742|RENAME_NEW_NAME|74620|285|15721|2|archive|2|0
|0x00000000|0
0x03D6BD58|$RKXD1U3.jpg|64404824|2015-03-24 20:11:42.8361742|CLOSE+RENAME_NEW_NAME|74620|285|15721|2|archi
ve|2|0|0x00000000|0
0x03D6BDB0|$RKXD1U3.jpg|64404912|2015-03-24 20:11:42.8361742|SECURITY_CHANGE|74620|285|15721|2|archive|2|0
|0x00000000|0
0x03D6BE08|$RKXD1U3.jpg|64405000|2015-03-24 20:11:42.8361742|CLOSE+SECURITY_CHANGE|74620|285|15721|2|archi
ve|2|0|0x00000000|0
```

Scenario 2

– Install *usncarve* tool (note we have changed the path)

```
                                                                    /bin/bash 101x24
root@kali:~/lab#
root@kali:~/lab# pip install usncarve
Collecting usncarve
  Downloading https://files.pythonhosted.org/packages/80/
2858556680cf9861f86/usncarve-1.2.2.tar.gz
Building wheels for collected packages: usncarve
  Running setup.py bdist_wheel for usncarve ... done
  Stored in directory: /root/.cache/pip/wheels/f7/f3/ea/2
d3af0
Successfully built usncarve
Installing collected packages: usncarve
Successfully installed usncarve-1.2.2
root@kali:~/lab#
```

– Verify installation

– Install usnparser tool

```
root@kali:~/lab#
root@kali:~/lab# pip install usnparser
Collecting usnparser
  Downloading https://files.pythonhosted.org/packages/d
79ea5f41cbaf92726dc/usnparser-4.0.3.tar.gz
Building wheels for collected packages: usnparser
  Running setup.py bdist_wheel for usnparser ... done
  Stored in directory: /root/.cache/pip/wheels/49/a4/ad
7db84
Successfully built usnparser
Installing collected packages: usnparser
Successfully installed usnparser-4.0.3
root@kali:~/lab#
```

```
┌──(kali㉿kali)-[~/lab6]
└─# pip3 install usnparser
Collecting usnparser
  Downloading usnparser-4.1.5.tar.gz (6.1 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Building wheels for collected packages: usnparser
  Building wheel for usnparser (pyproject.toml) ... done
  Created wheel for usnparser: filename=usnparser-4.1.5-py3-none-any.whl size
=5617 sha256=aee6d75195ce8e4cbf351921cbd49fc06217f833767f315684a7264caf9d114c
  Stored in directory: /root/.cache/pip/wheels/c9/8d/4d/3384811dedf2dd3fff3e6
1e45f5428ff8d83e6543916e5af36
Successfully built usnparser
Installing collected packages: usnparser
Successfully installed usnparser-4.1.5
```

– Verify installation

```
root@kali:~/lab#
root@kali:~/lab# usn.py -h
usage: usn.py [-h] [-b] [-c] -f FILE -o OUTFILE [-s SYSTEM] [-t] [-v]

optional arguments:
  -h, --help            show this help message and exit
  -b, --body            Return USN records in comma-separated format
  -c, --csv             Return USN records in comma-separated format
  -f FILE, --file FILE  Parse the given USN journal file
  -o OUTFILE, --outfile OUTFILE
                        Parse the given USN journal file
  -s SYSTEM, --system SYSTEM
                        System name (use with -t)
  -t, --tln             TLN ou2tput (use with -s)
  -v, --verbose         Return all USN properties for each record (JSON)
root@kali:~/lab#
```

```
┌──(kali㉿kali)-[~/lab6]
└─# usn.py -h
usage: usn.py [-h] [-b] [-c] -f FILE -o OUTFILE [-s SYSTEM] [-t] [-v]

options:
  -h, --help            show this help message and exit
  -b, --body            Return USN records in comma-separated format
  -c, --csv             Return USN records in comma-separated format
  -f, --file FILE       Parse the given USN journal file
  -o, --outfile OUTFILE
                        Parse the given USN journal file
  -s, --system SYSTEM   System name (use with -t)
  -t, --tln             TLN ou2tput (use with -s)
  -v, --verbose         Return all USN properties for each record (JSON)
```

– *usncarve.py -f* input file *-o* output file


```
/bin/bash 101x24
root@kali:~/lab#
root@kali:~/lab# usncarve.py -f cfreds_2015_data_leakage_pc.dd -o usn.raw
root@kali:~/lab#
root@kali:~/lab# ls -l usn.raw
-rw-r--r-- 1 root root 46465030 Nov 25 20:06 usn.raw
root@kali:~/lab#
```

```
┌──(kali㉿kali)-[~/lab6]
└─# usncarve.py -f cfreds_2015_data_leakage_pc.dd -o usn.raw

┌──(kali㉿kali)-[~/lab6]
└─# ls -l usn.raw
-rw-r--r-- 1 root root 46465030 Jun 19 07:17 usn.raw
```

– *usn.py -f* input file *-o* output file


```
/bin/bash 101x24
root@kali:~/lab#
root@kali:~/lab# usn.py -f usn.raw -o usn.csv
root@kali:~/lab#
root@kali:~/lab# ls -l usn.csv
-rw-r--r-- 1 root root 40899888 Nov 25 20:08 usn.csv  ←
root@kali:~/lab#
```

```
┌──(kali㉿kali)-[~/lab6]
└─# usn.py -f usn.raw -o usn.csv
/root/lab/venv/bin/usn.py:139: DeprecationWarning: datetime.datetime.utcfromt
imestamp() is deprecated and scheduled for removal in a future version. Use t
imezone-aware objects to represent datetimes in UTC: datetime.datetime.fromti
mestamp(timestamp, datetime.UTC).
  return str(datetime.utcfromtimestamp(float(filetime) * 1e-7 - 11644473600))

┌──(kali㉿kali)-[~/lab6]
└─# ls -l usn.csv
-rw-r--r-- 1 root root 40899888 Jun 19 07:19 usn.csv
```

– View renamed files

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Save the document with the filename "**YOUR NAME Lab 6.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 6 From YOUR NAME**", replacing "YOUR NAME" with your real name.