

Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

Lớp: IA1901

Lab 6: Update Sequence Number (USN) Journaling

Scenario 1

Install UsnJrnl2Csv tool -> Run UsnJrnl2.exe to covert UsnJrnl.bin to .csv:

```
(dungthe190680@dungthe190680) [~/Lab]
$ git clone https://github.com/jschicht/UsnJrnl2Csv.git
Cloning into 'UsnJrnl2Csv'...
remote: Enumerating objects: 182, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 182 (delta 0), reused 2 (delta 0), pack-reused 176 (from 1)
Receiving objects: 100% (182/182), 12.96 MiB | 3.03 MiB/s, done.
Resolving deltas: 100% (111/111), done.

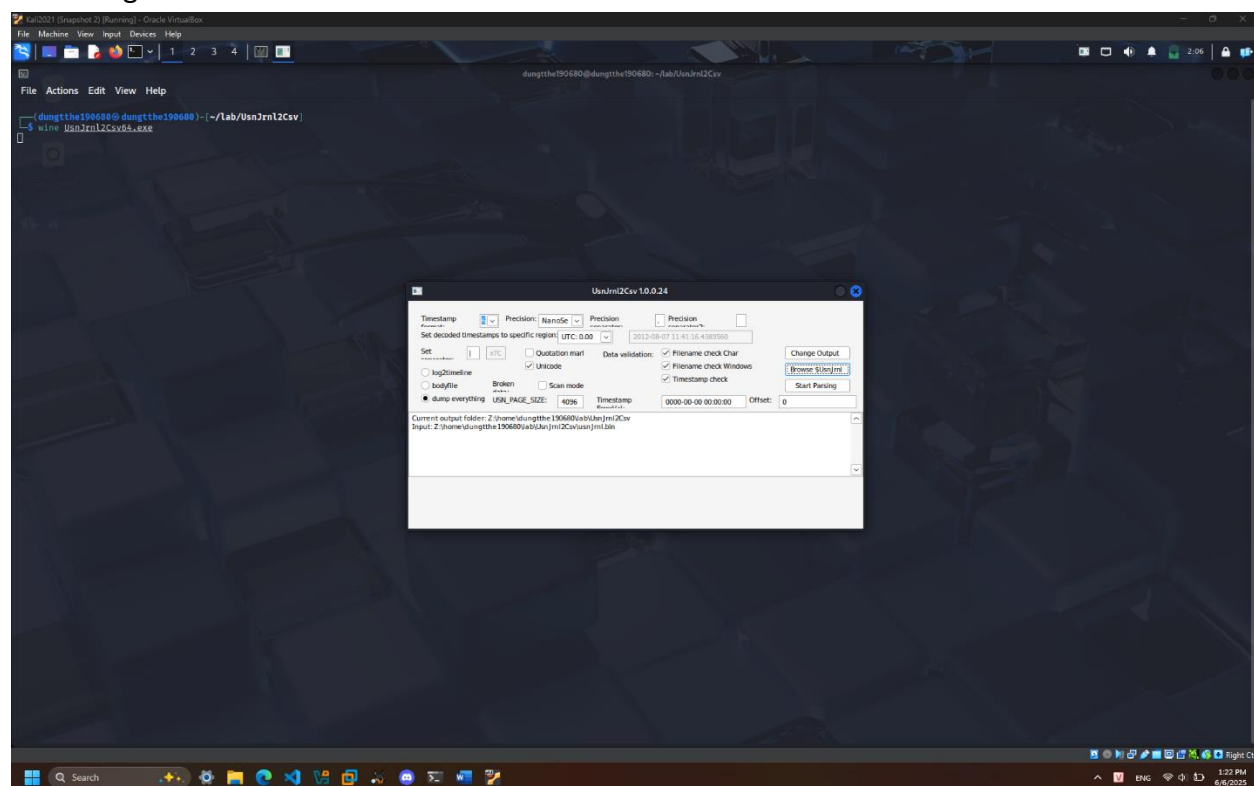
(dungthe190680@dungthe190680) [~/Lab]
$ cat -i raw -o 286848 cfreds_2015_data_leakage_pc.dd 59816-128-3 > UsnJrnl2Csv/usnJrnl.bin

(dungthe190680@dungthe190680) [~/Lab]
$ ls UsnJrnl2Csv/usnJrnl.bin -l
-rw-rw-r-- 1 dungthe190680 dungthe190680 69767168 Jun  6 00:24 UsnJrnl2Csv/usnJrnl.bin

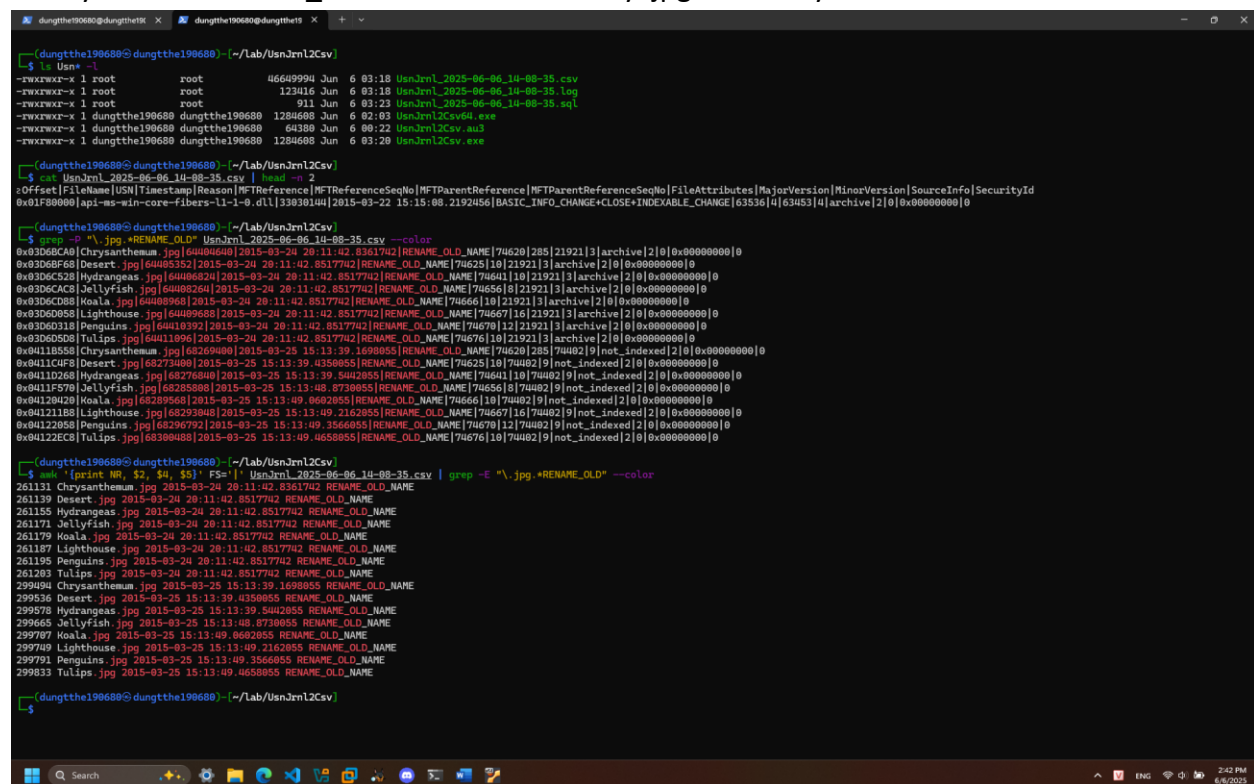
(dungthe190680@dungthe190680) [~/Lab]
$ cd UsnJrnl2Csv

(dungthe190680@dungthe190680) [~/Lab/UsnJrnl2Csv]
$
```

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:



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

```
(dungttthe190680@dungttthe190680) ~[/Lab/UsnJrn12Csv]
$ grep "2015-03-24 20:11:42.8361742" UsnJrn1_2025-06-06_10-08-35.csv
0x03060000|Chrystiantheman.jpg|64404736|2015-03-24 20:11:42.8361742|RENAME_OLD_NAME|74620|285|15721|3|archive|2|0|0x00000000|0
0x03060000|$RHXDIU3.jpg|64404736|2015-03-24 20:11:42.8361742|RENAME_NEW_NAME|74620|285|15721|2|archive|2|0|0x00000000|0
0x03060000|$RHXDIU3.jpg|64404824|2015-03-24 20:11:42.8361742|CLOSE+RENAME_NEW_NAME|74620|285|15721|2|archive|2|0|0x00000000|0
0x03060000|$RHXDIU3.jpg|64404912|2015-03-24 20:11:42.8361742|SECURITY_CHANGE|74620|285|15721|2|archive|2|0|0x00000000|0
0x03060000|$RHXDIU3.jpg|64405000|2015-03-24 20:11:42.8361742|CLOSE+SECURITY_CHANGE|74620|285|15721|2|archive|2|0|0x00000000|0
(dungttthe190680@dungttthe190680) ~[/Lab/UsnJrn12Csv]
$
```

Scenario 2

Install usncarve tool -> Verify installation -> Install usnparser tool -> Verify installation:

```
(dungttthe190680@dungttthe190680) ~[/Lab]
$ pipx install usncarve
'usncarve' already seems to be installed. Not modifying existing installation in
'/home/dungttthe190680/.local/share/pipx/venvs/usncarve'. Pass '--force' to force installation.
(dungttthe190680@dungttthe190680) ~[/Lab]
$ usncarve.py -h
usage: usncarve.py [-h] -f FILE -o OUTFILE

options:
  -h, --help            show this help message and exit
  -f, --file FILE        Carve USN records from the given file
  -o, --outfile OUTFILE  Output to the given file

(dungttthe190680@dungttthe190680) ~[/Lab]
$ pipx install usnparser
'usnparser' already seems to be installed. Not modifying existing installation in
'/home/dungttthe190680/.local/share/pipx/venvs/usnparser'. Pass '--force' to force installation.
(dungttthe190680@dungttthe190680) ~[/Lab]
$ 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 output (use with -s)
  -v, --verbose         Return all USN properties for each record (JSON)

(dungttthe190680@dungttthe190680) ~[/Lab]
$ usncarve.py -f cfreds_2015_data_leakage_pc.dd -o usn.raw
(dungttthe190680@dungttthe190680) ~[/Lab]
$ ls -l usn.raw
-rw-rw-r-- 1 dungttthe190680 dungttthe190680 46465030 Jun  6 04:10 usn.raw
(dungttthe190680@dungttthe190680) ~[/Lab]
$ usn.py -f usn.raw -o usn.csv
(dungttthe190680@dungttthe190680) ~[/Lab]
$ ls -l usn.csv
-rw-rw-r-- 1 dungttthe190680 dungttthe190680 43344948 Jun  6 04:11 usn.csv
(dungttthe190680@dungttthe190680) ~[/Lab]
$
```

View renamed files:

```
(dungtthe190680@dungtthe190680) [~/Lab]
$ cat usn.csv | grep -i rename | head
2015-03-22 15:14:17.097954+00:00 | edb0043D.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-22 15:14:17.097954+00:00 | edbtap.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_NEW_NAME
2015-03-22 15:14:17.097954+00:00 | edbtap.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_NEW_NAME CLOSE
2015-03-22 15:14:17.097954+00:00 | edb.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-22 15:14:17.097954+00:00 | edb0044E.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_NEW_NAME
2015-03-22 15:14:17.097954+00:00 | edb0044E.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_NEW_NAME CLOSE
2015-03-22 15:14:17.113554+00:00 | edbtap.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-22 15:14:17.113554+00:00 | edb.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_NEW_NAME
2015-03-22 15:14:17.113554+00:00 | edb.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_NEW_NAME CLOSE
2015-03-22 15:14:18.174358+00:00 | edb.log | ARCHIVE NOT_CONTENT_INDEXED | RENAME_OLD_NAME

(dungtthe190680@dungtthe190680) [~/Lab]
$ cat usn.csv | grep -i rename | wc -l
45
grep: (standard input): binary file matches

(dungtthe190680@dungtthe190680) [~/Lab]
$ grep --text -P "\.jpg.*RENAME_OLD" usn.csv --color
2015-03-25 15:13:39.169804+00:00 | Chrysanthemum.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:39.463803+00:00 | Desert.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:39.544205+00:00 | Hydrangeas.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:48.873805+00:00 | Jellyfish.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:49.066204+00:00 | Koala.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:49.216204+00:00 | Lighthouse.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:49.356604+00:00 | Penguins.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:49.465805+00:00 | Tulips.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-24 20:11:42.836174+00:00 | Chrysanthemum.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Desert.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Hydrangeas.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Jellyfish.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Koala.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Lighthouse.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Penguins.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Tulips.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.836174+00:00 | Chrysanthemum.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Desert.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Hydrangeas.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Jellyfish.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Koala.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Lighthouse.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Penguins.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-24 20:11:42.851774+00:00 | Tulips.jpg | ARCHIVE | RENAME_OLD_NAME
2015-03-25 15:13:40.066204+00:00 | Koala.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:49.216204+00:00 | Lighthouse.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:49.356604+00:00 | Penguins.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:49.465805+00:00 | Tulips.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:39.169804+00:00 | Chrysanthemum.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:39.435803+00:00 | Desert.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:39.544205+00:00 | Hydrangeas.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME
2015-03-25 15:13:48.873805+00:00 | Jellyfish.jpg | NOT_CONTENT_INDEXED | RENAME_OLD_NAME

(dungtthe190680@dungtthe190680) [~/Lab]
$
```