Cyber Law and Forensics (CS402)

Practical Exam (26-Apr-2023)

**U19CS012**

A.) Answer the Following Questions from the Given Evidence Files:

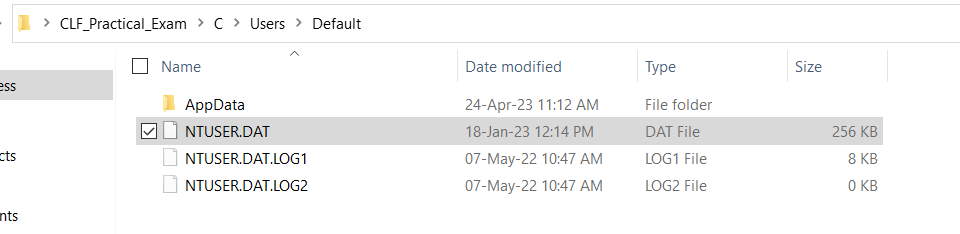
(1) Identify the commands that were typed in RUN dialogue box.

HKCU(ntuser.dat)\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

-> **\RunMRU** Shows MRU (Most Recent Used) run command

1. Default – Nothing Found

(C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Users\Default)



2. HP - Found

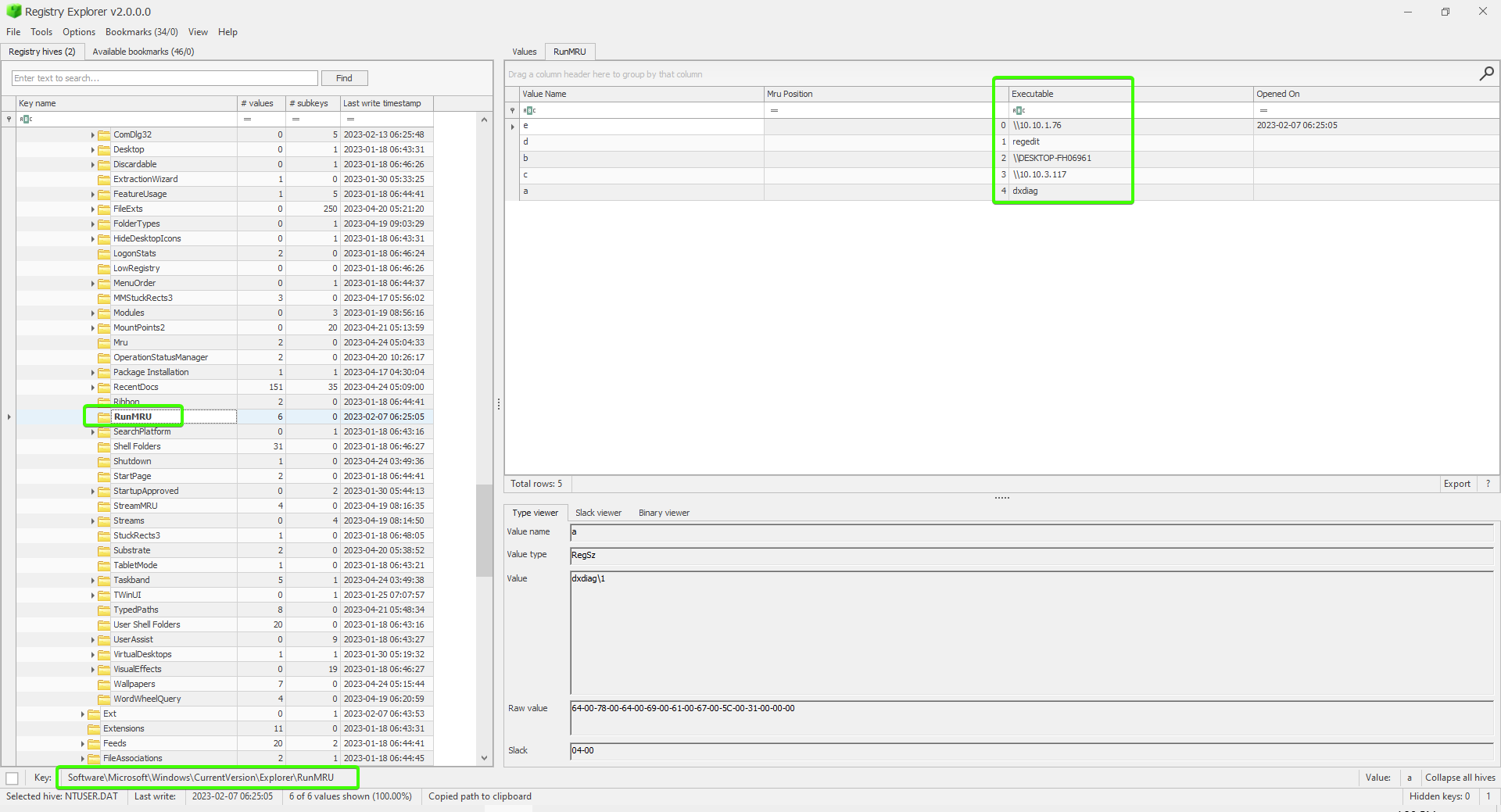
**Tool Used**:

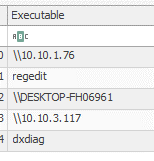
Registry Explorer by Eric Zimmerman

**File Used**:

NTUSER.DAT

**Location**: C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Users\HP\NTUSER.DAT

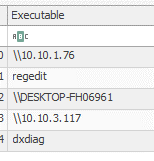




**Path**

Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

**Final Answer**:



(2) When the log\_tempering.csv was last opened?

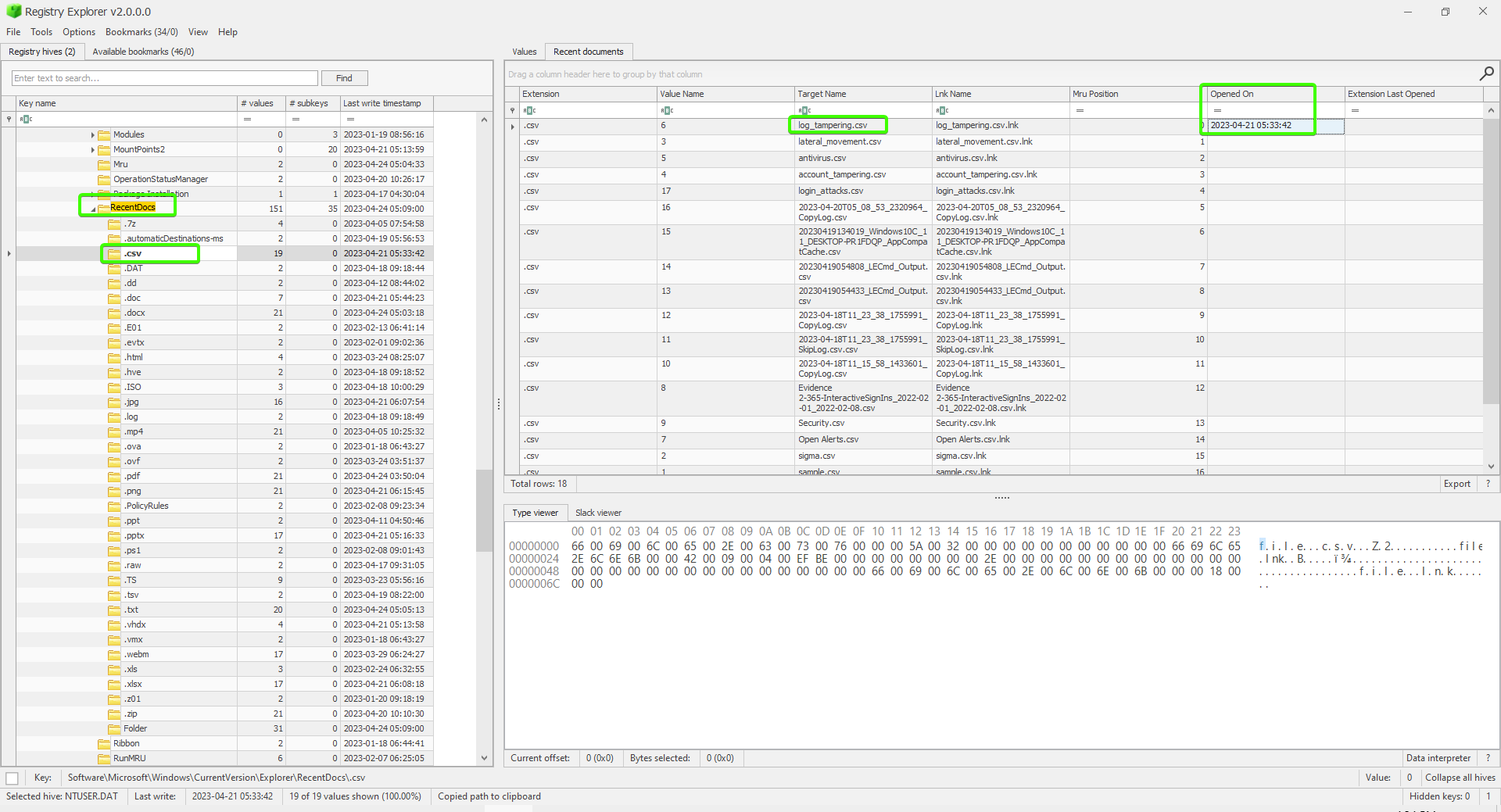
**Tool Used**:

Registry Explorer by Eric Zimmerman

**File Used**:

NTUSER.DAT

**Location**: C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Users\HP\NTUSER.DAT



**Path**

System (HKLM) \ Software \ Microsoft \ Windows \ Current Version \ RecentDocs

**Final Answer**:



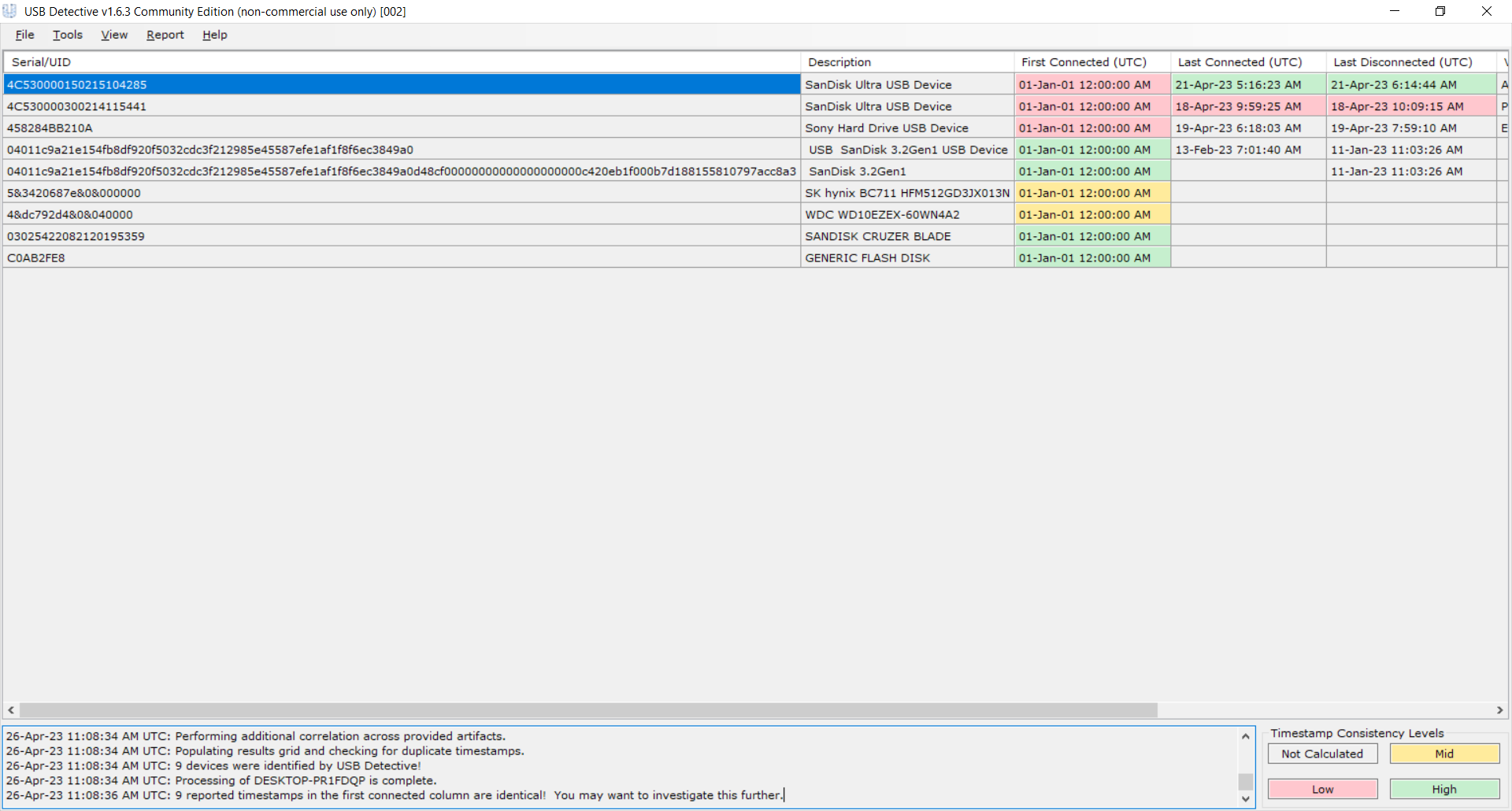
(3) Identify USB devices attached to the system.

**Tool Used**:

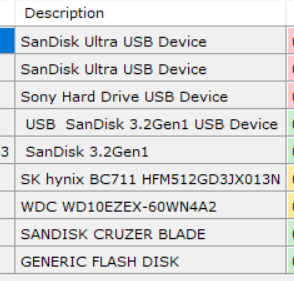
USB Detective

**File Used**:

1. SYSTEM Hive (C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Windows\System32\config)
2. SOFTWARE Hive (C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Windows\System32\config)
3. NTUSER.DAT Hive (C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Users\HP)
4. Setupapi Log (C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Windows\INF)
5. Amcache Hive (C:\Users\Admin\Desktop\CLF\_Practical\_Exam\C\Windows\AppCompat\Programs)



**Final Answer**:



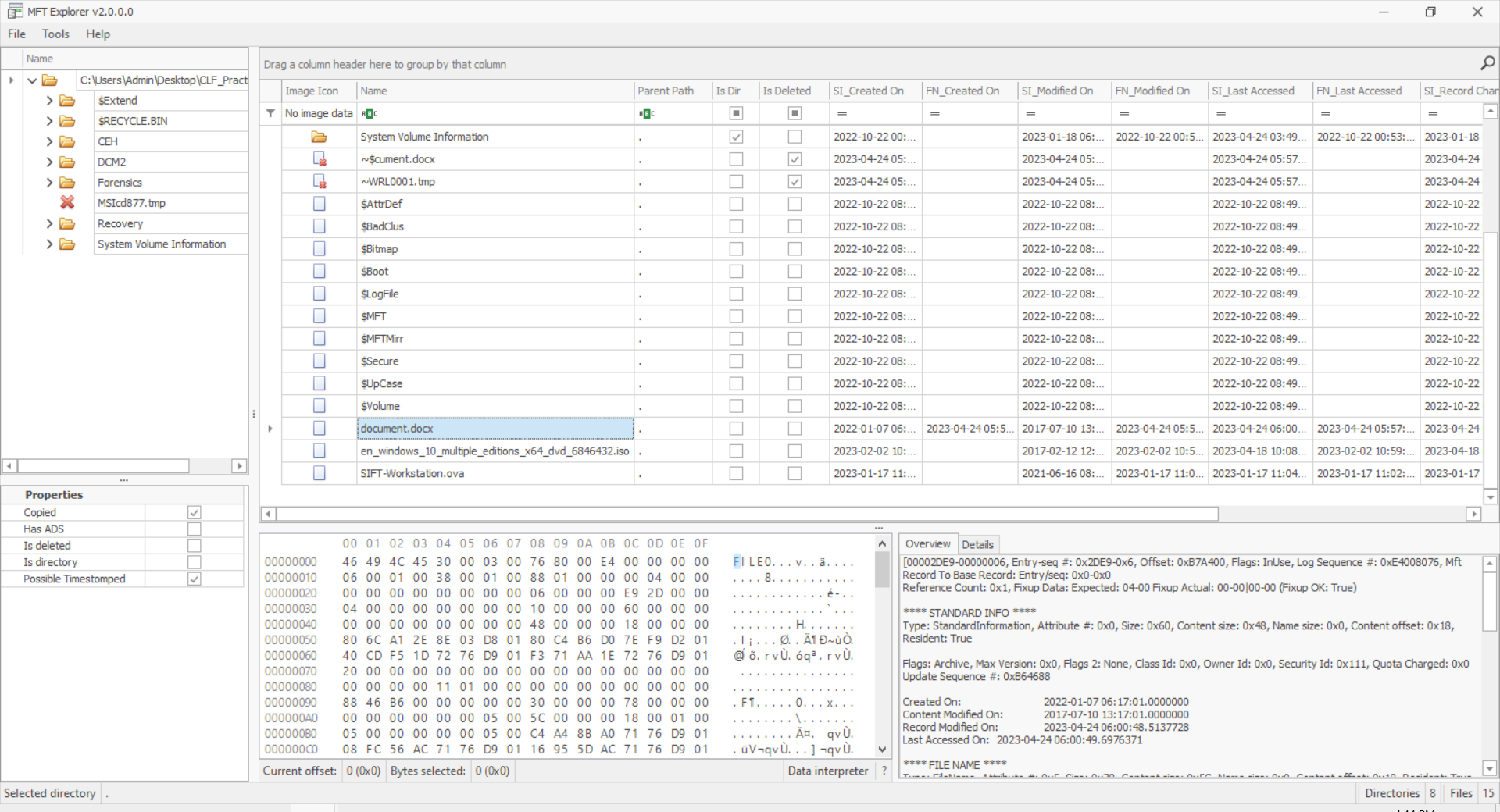
(4) Identify the file having manipulated time stamp.

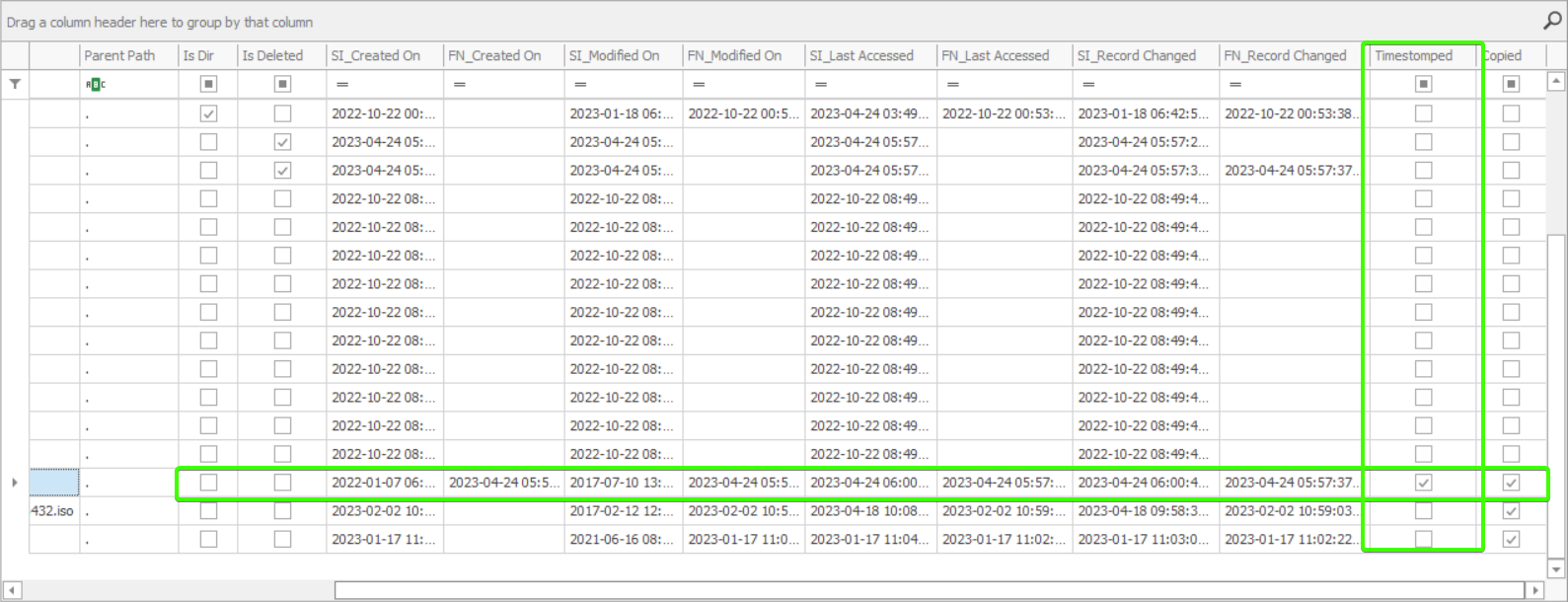
**Tool Used**:

MFT Explorer

**File Used**:

MFT File



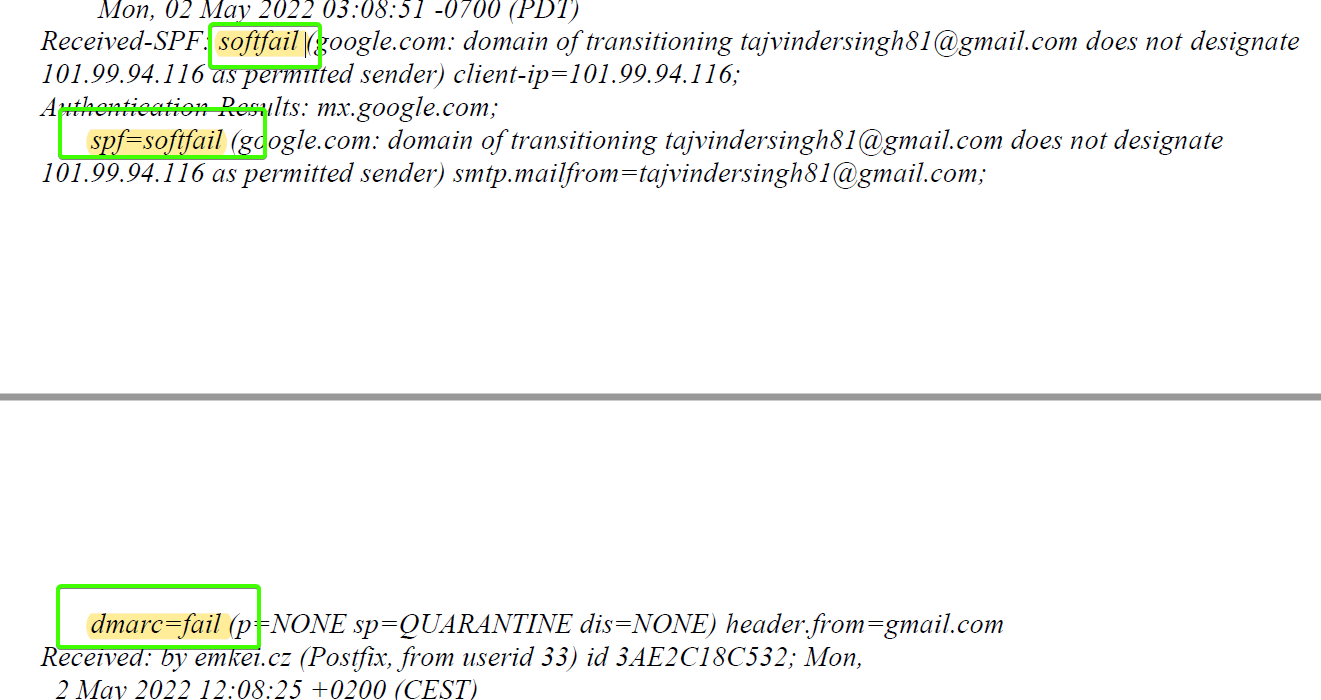


**Final Answer**:

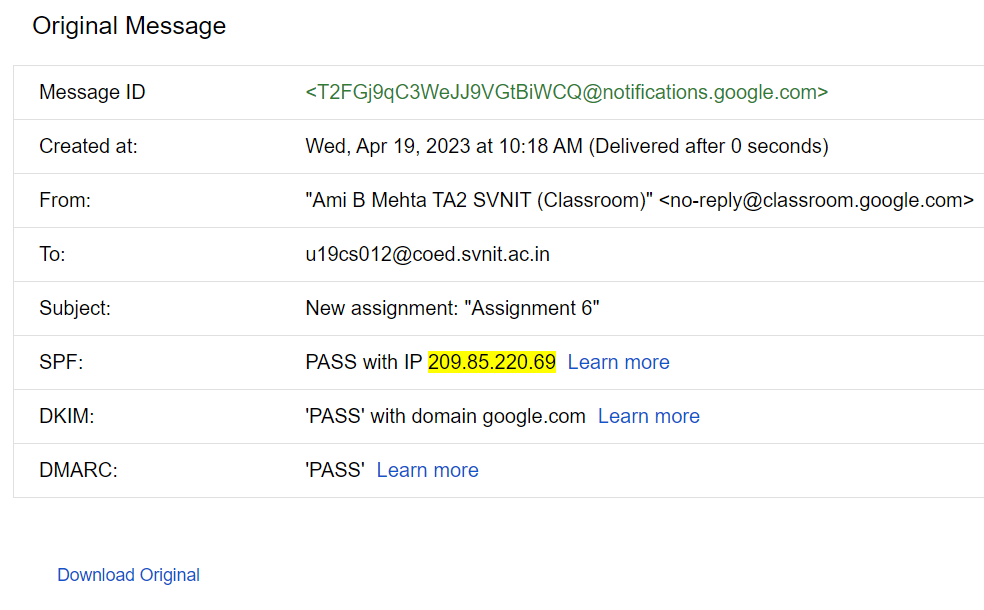


(5) Following is the email header. Analyse the header and identify whether it is legitimate or not. If not, from where it was sent.

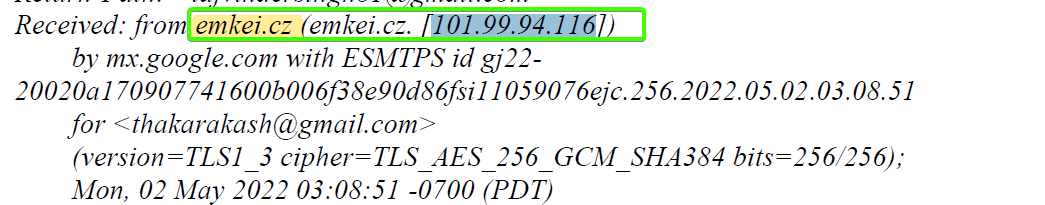
The Given Email is **Not Legitimate / Fake.**

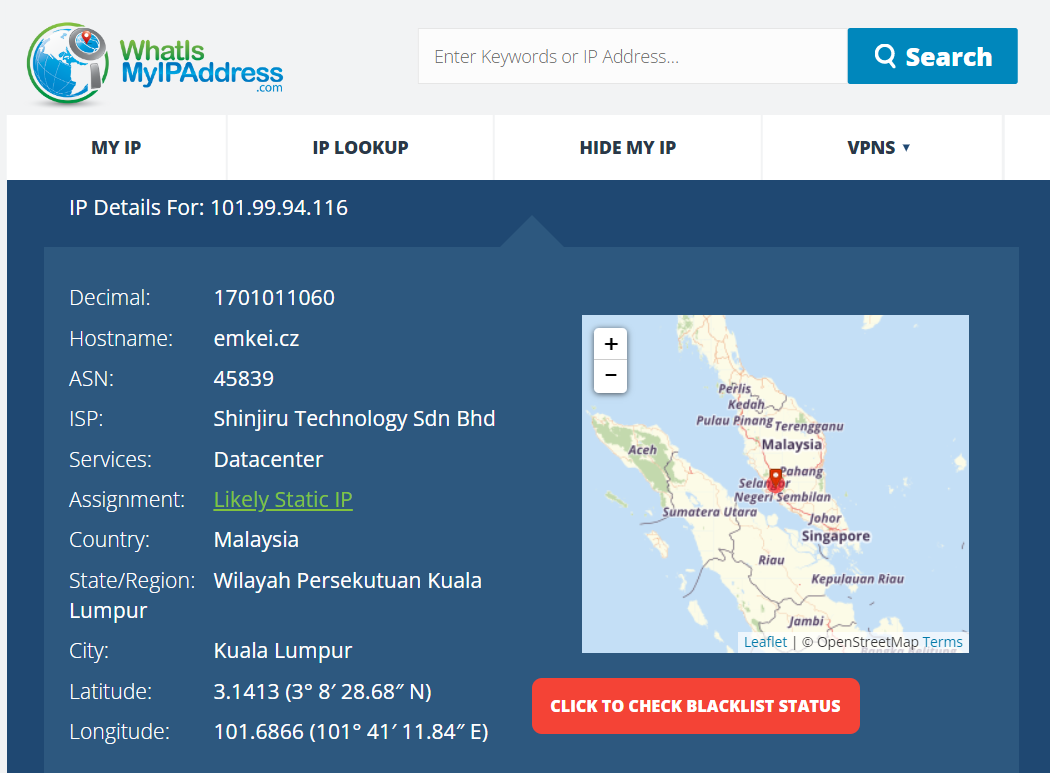


* Email Evidence is in Email itself (Header)!
* Tracing -> Examination of an Email Header to determine its **point of origin**



Ideally, It should pass all SPF, DKIM & DMARC.





**Sent Location:**

Country:Malaysia

State/Region:Wilayah Persekutuan Kuala Lumpur

City:Kuala Lumpur

Latitude:3.1413 (3° 8′ 28.68″ N)

Longitude:101.6866 (101° 41′ 11.84″ E)

**SUBMITTED BY**:

U19CS012

BHAGYA VINOD RANA