vishwaCTF

CHALLENGE NAME : [SMOKE OUT THE RAT]

DEV : [SAKSHAM SAIPATWAR]

CATEGORY : [DIGITAL FORENSICS]

LEVEL : [EASY]

2024

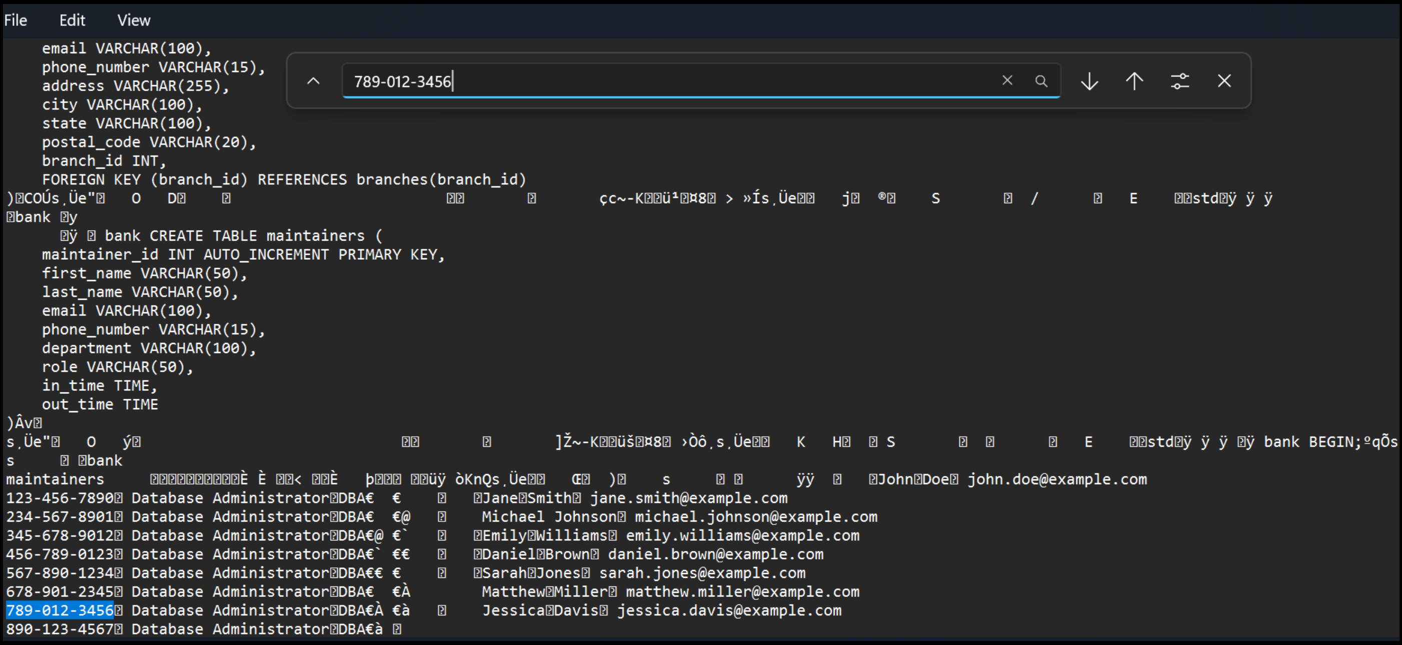
CHALLENGE NAME : [SMOKE OUT THE RAT]

Description :- There was a major heist at the local bank. Initial findings suggest that an intruder from within the bank, specifically someone from the bank's database maintenance team, aided in the robbery. This traitor granted access to an outsider, who orchestrated the generation of fake transactions and the depletion of our valuable customers' accounts. We have the phone number, '789-012-3456', from which the login was detected, which manipulated the bank's employee data. Additionally, it's noteworthy that this intruder attempted to add gibberish to the binlog and ultimately dropped the entire database at the end of the heist.

Your task is to identify the first name of the traitor, the last name of the outsider, and the time at which the outsider was added to the database.

Flag format :
VishwaCTF{TraitorFirstName_OutsiderLastName_HH:MM:SS}

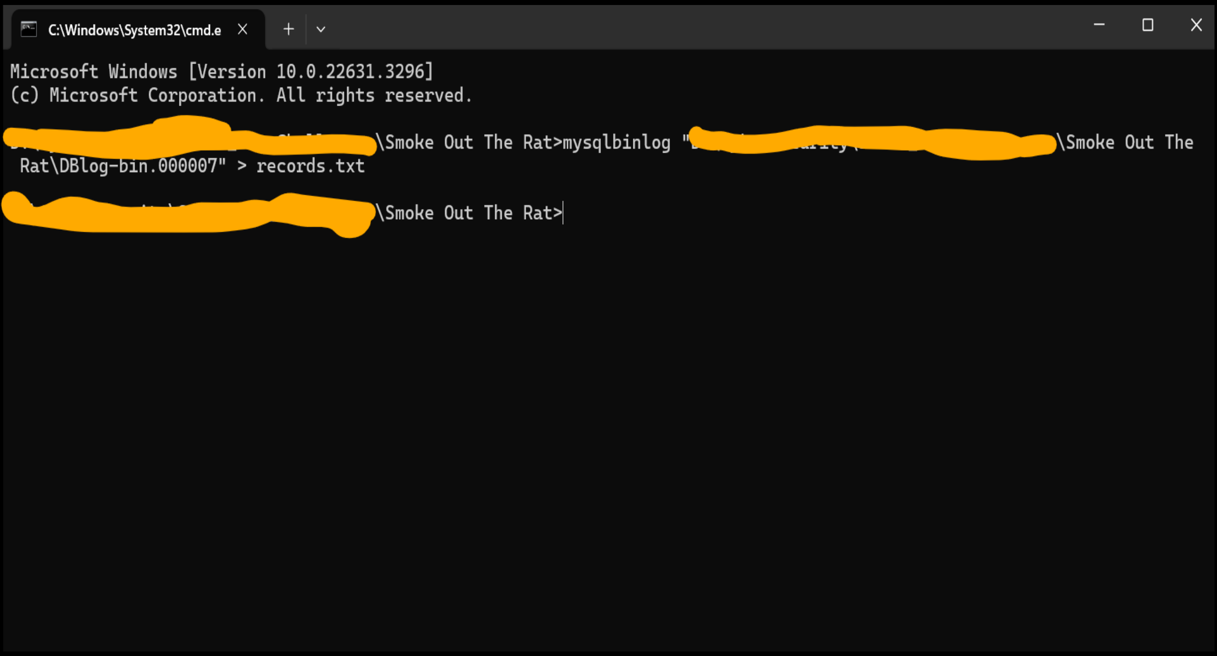
Step 1 : *Find the traitor using the phone number given . You get the first name as 'Matthew'.*



```
    email VARCHAR(100),
    phone_number VARCHAR(15),
    address VARCHAR(255),
    city VARCHAR(100),
    state VARCHAR(100),
    postal_code VARCHAR(20),
    branch_id INT,
    FOREIGN KEY (branch_id) REFERENCES branches(branch_id)
)□COÚs¸Üe"□   O   D□    □                         □□       □       çc~-K□□ü¹□¤8□ > »Ís¸Üe□□   j□  ®□    S       □  /      □   E    □□std□ÿ ÿ ÿ
□bank □y
      □ÿ □ bank CREATE TABLE maintainers (
    maintainer_id INT AUTO_INCREMENT PRIMARY KEY,
    first_name VARCHAR(50),
    last_name VARCHAR(50),
    email VARCHAR(100),
    phone_number VARCHAR(15),
    department VARCHAR(100),
    role VARCHAR(50),
    in_time TIME,
    out_time TIME
)Âv□
s¸Üe"□   O   ý□                         □□       □       ]Ž~-K□□üš□¤8□ ›Òô¸s¸Üe□□   K   H□  □ S       □  □       □   E    □□std□ÿ ÿ ÿ □ÿ bank BEGIN;ºqÕs
s      □ □bank
maintainers     □□□□□□□□□□È È □□< □□È   þ□□□ □□üÿ òKnQs¸Üe□□   Œ□  )□    s     □ □      ÿÿ  □   □John□Doe□ john.doe@example.com
123-456-7890□ Database Administrator□DBA€  €    □   □Jane□Smith□ jane.smith@example.com
234-567-8901□ Database Administrator□DBA€  €@   □    Michael Johnson□ michael.johnson@example.com
345-678-9012□ Database Administrator□DBA€@ €`   □   □Emily□Williams□ emily.williams@example.com
456-789-0123□ Database Administrator□DBA€` €€   □   □Daniel□Brown□ daniel.brown@example.com
567-890-1234□ Database Administrator□DBA€€ €    □   □Sarah□Jones□ sarah.jones@example.com
678-901-2345□ Database Administrator□DBA€  €À        Matthew□Miller□ matthew.miller@example.com
789-012-3456□ Database Administrator□DBA€À €à   □    Jessica□Davis□ jessica.davis@example.com
890-123-4567□ Database Administrator□DBA€à □
```

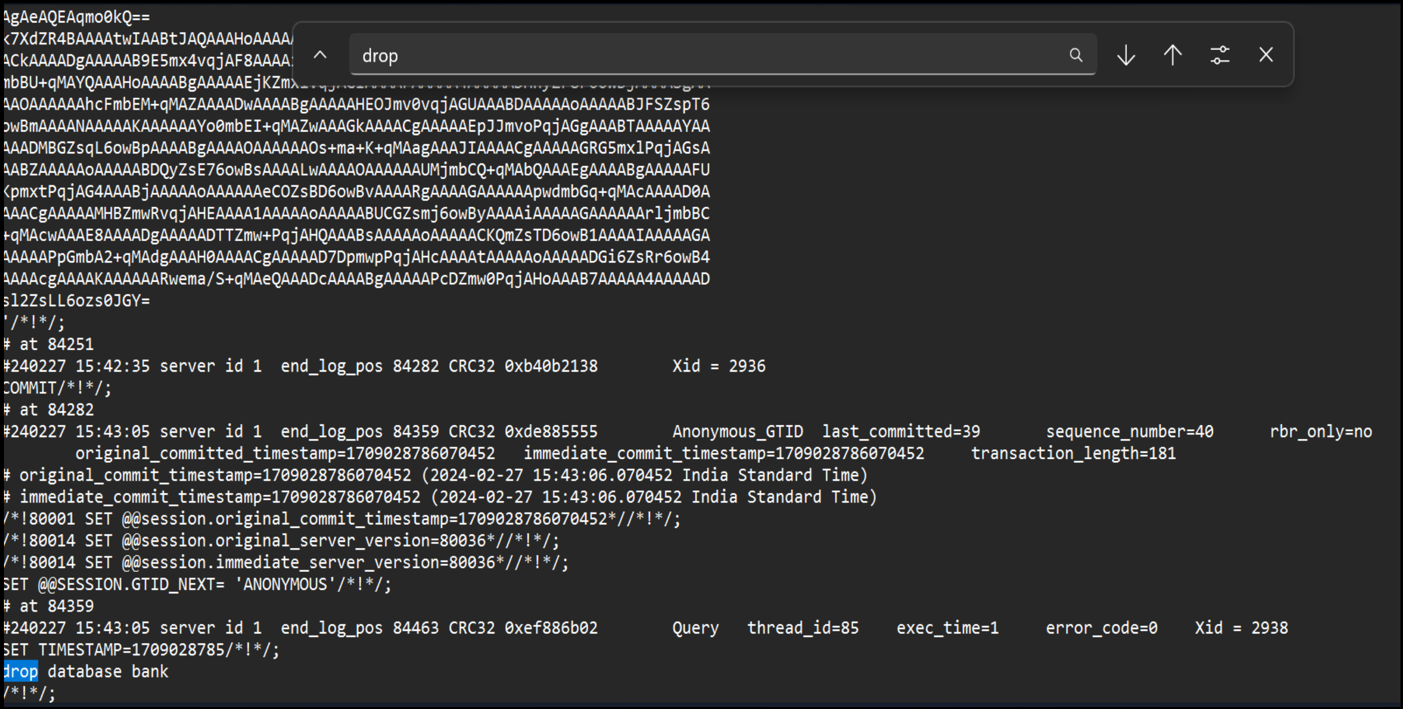
Note : Analyse the database log carefully , look for things which describe the database like tables , columns and other to get an basic Idea about what the database is all about , it will benefit you getting the flag .

Step 2 : Now as you are asked about the timestamp , you need to convert the binary into readable format . The which helps you achieving this 'mysqlbinlog' utility .



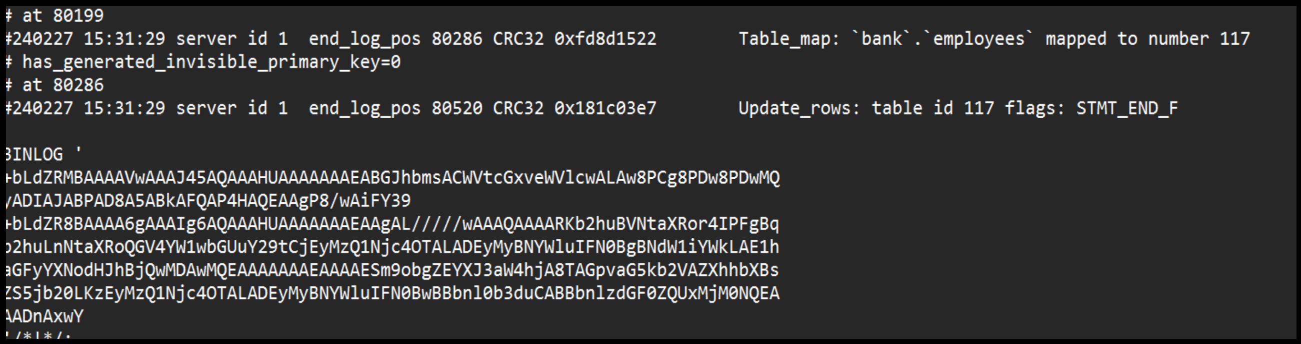
```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

[redacted]\Smoke Out The Rat>mysqlbinlog "[redacted]\Smoke Out The
Rat\DBlog-bin.000007" > records.txt

[redacted]\Smoke Out The Rat>
```

Step 3 : Now open the decrypted text file , and get the remaining part of the flag . The description hints that , outsider added in the database created fake transactions and ultimately dropped the entire database . Find the 'drop' statement and search nearby …



```
AgAeAQEAqmo0kQ==
<7XdZR4BAAAAtwIAABtJAQAAAHoAAAA
ACkAAAADgAAAAAB9E5mx4vqjAF8AAAA
mbBU+qMAYQAAAHoAAAABgAAAAAEjKZmx
AAOAAAAAAhcFmbEM+qMAZAAAADwAAAABgAAAAAHEOJmv0vqjAGUAAABDAAAAAoAAAAABJFSZspT6
owBmAAAANAAAAAKAAAAAAYo0mbEI+qMAZwAAAGkAAAACgAAAAAEpJJmvoPqjAGgAAABTAAAAAYAA
AAADMBGZsqL6owBpAAAABgAAAAOAAAAAAOs+ma+K+qMAagAAAJIAAAACgAAAAAGRG5mxlPqjAGsA
AABZAAAAAoAAAAABDQyZsE76owBsAAAALwAAAAOAAAAAAUMjmbCQ+qMAbQAAAEgAAAABgAAAAAFU
<pmxtPqjAG4AAABjAAAAAoAAAAAAeCOZsBD6owBvAAAARgAAAAGAAAAAApwdmbGq+qMAcAAAAD0A
AAACgAAAAAMHBZmwRvqjAHEAAAA1AAAAAoAAAAABUCGZsmj6owByAAAAiAAAAAGAAAAAArljmbBC
+qMAcwAAAE8AAAADgAAAAADTTZmw+PqjAHQAAABsAAAAAoAAAAACKQmZsTD6owB1AAAAIAAAAAGA
AAAAAPpGmbA2+qMAdgAAAH0AAAACgAAAAAD7DpmwpPqjAHcAAAAtAAAAAoAAAAADGi6ZsRr6owB4
AAAAcgAAAAKAAAAAARwema/S+qMAeQAAADcAAAABgAAAAAPcDZmw0PqjAHoAAAB7AAAAA4AAAAAD
sl2ZsLL6ozs0JGY=
'/*!*/;
# at 84251
#240227 15:42:35 server id 1  end_log_pos 84282 CRC32 0xb40b2138        Xid = 2936
COMMIT/*!*/;
# at 84282
#240227 15:43:05 server id 1  end_log_pos 84359 CRC32 0xde885555        Anonymous_GTID  last_committed=39       sequence_number=40      rbr_only=no
        original_committed_timestamp=1709028786070452   immediate_commit_timestamp=1709028786070452     transaction_length=181
# original_commit_timestamp=1709028786070452 (2024-02-27 15:43:06.070452 India Standard Time)
# immediate_commit_timestamp=1709028786070452 (2024-02-27 15:43:06.070452 India Standard Time)
/*!80001 SET @@session.original_commit_timestamp=1709028786070452*//*!*/;
/*!80014 SET @@session.original_server_version=80036*//*!*/;
/*!80014 SET @@session.immediate_server_version=80036*//*!*/;
SET @@SESSION.GTID_NEXT= 'ANONYMOUS'/*!*/;
# at 84359
#240227 15:43:05 server id 1  end_log_pos 84463 CRC32 0xef886b02        Query   thread_id=85    exec_time=1     error_code=0    Xid = 2938
SET TIMESTAMP=1709028785/*!*/;
drop database bank
/*!*/;
```

Step 4 : Scrolling a bit you can see an update made in the employees table , note the timestamp , and converting the binlog using Base64 helps you get the name of the outsider added .



```
# at 80199
#240227 15:31:29 server id 1  end_log_pos 80286 CRC32 0xfd8d1522       Table_map: `bank`.`employees` mapped to number 117
# has_generated_invisible_primary_key=0
# at 80286
#240227 15:31:29 server id 1  end_log_pos 80520 CRC32 0x181c03e7       Update_rows: table id 117 flags: STMT_END_F

BINLOG '
+bLdZRMBAAAAVwAAAJ45AQAAAHUAAAAAAAAEABGJhbmsACWVtcGxveWVlcwALAw8PCg8PDw8PDwMQ
/ADIAJABPAD8A5ABkAFQAP4HAQEAAgP8/wAiFY39
+bLdZR8BAAAA6gAAAIg6AQAAAHUAAAAAAAAEAAgAL/////wAAAQAAAARKb2huBVNtaXRor4IPFgBq
b2huLnNtaXRoQGV4YW1wbGUuY29tCjEyMzQ1Njc4OTALADEyMyBNYWluIFN0BgBNdW1iYWkLAE1h
aGFyYXNodHJhBjQwMDAwMQEAAAAAAAAEAAAAESm9obgZEYXJ3aW4hjA8TAGpvaG5kb2VAZXhhbXBs
ZS5jb20LKzEyMzQ1Njc4OTALADEyMyBNYWluIFN0BwBBbnl0b3duCABBbnlzdGF0ZQUxMjM0NQEA
AADnAxwY
'/*!*/;
```

FLAG :- *VishwaCTF{Matthew_Darwin_15:31:29}*