Simple MySQL Data Extraction

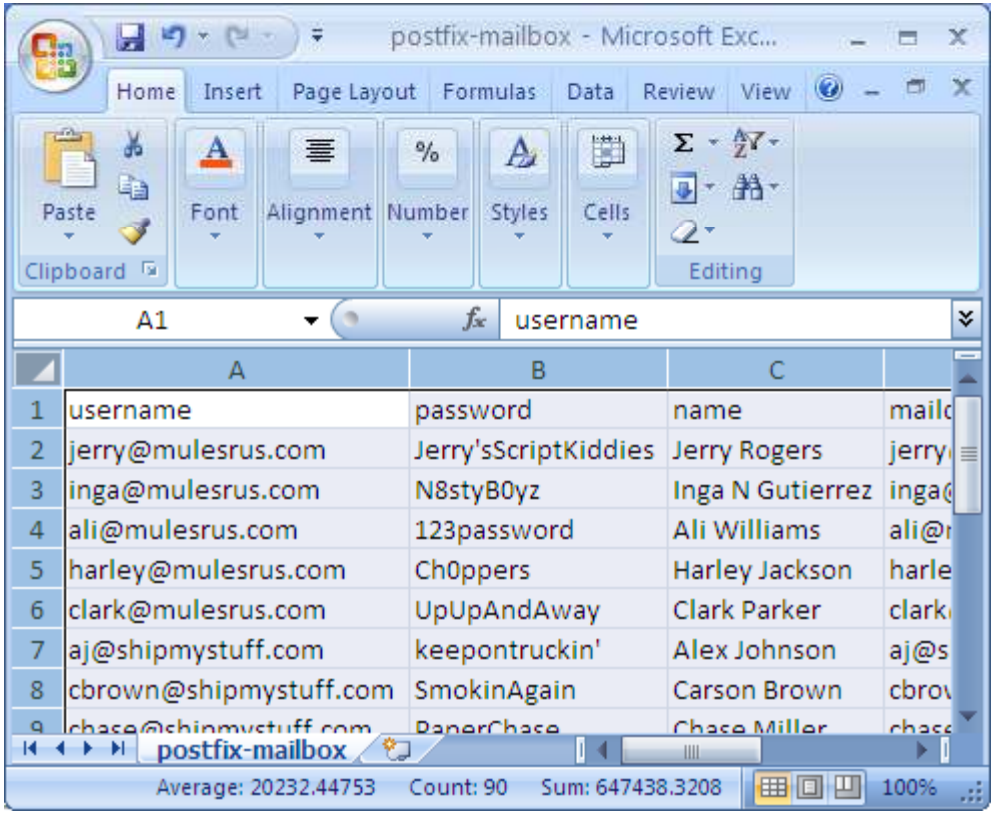
Hal Pomeranz

Deer Run Associates

Your Mission

Start with this…

… and end up with this:



	A	B	C	
1	username	password	name	mailc
2	jerry@mulesrus.com	Jerry'sScriptKiddies	Jerry Rogers	jerry
3	inga@mulesrus.com	N8styB0yz	Inga N Gutierrez	inga@
4	ali@mulesrus.com	123password	Ali Williams	ali@r
5	harley@mulesrus.com	Ch0ppers	Harley Jackson	harle
6	clark@mulesrus.com	UpUpAndAway	Clark Parker	clark
7	aj@shipmystuff.com	keepontruckin'	Alex Johnson	aj@s
8	cbrown@shipmystuff.com	SmokinAgain	Carson Brown	cbrov
9	chase@shipmystuff.com	PaperChase	Chase Miller	chase

What You'll Need

- Working copy of your evidence
- Tools to extract files/directories from evidence
- Analysis machine with working MySQL install

Overview of Process

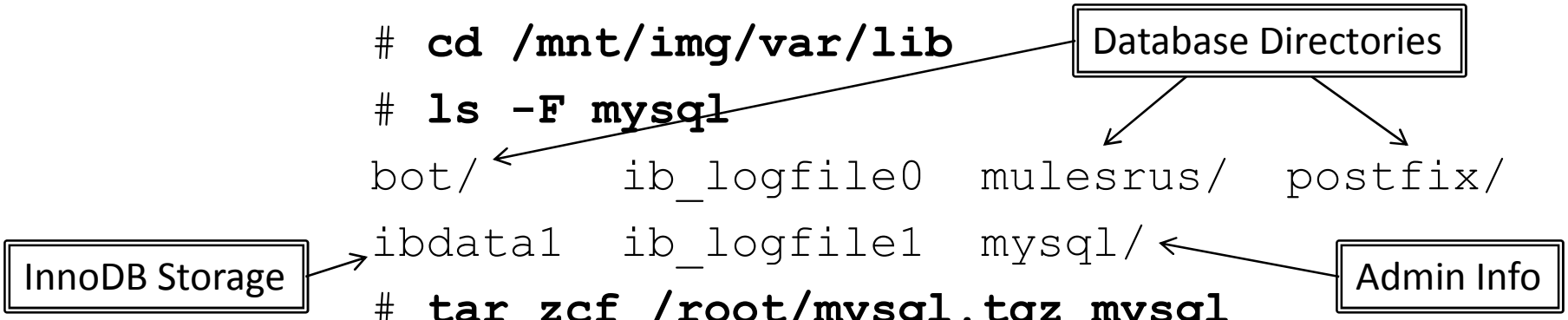
1. Extract database directories from evidence
2. Copy extracted data to MySQL on analysis host
3. Obtain access to extracted data
4. List databases/tables, investigate content
5. Write "interesting" data to Tab or CSV files

Step 1a: Where's the Data?

- Probably /var/lib/mysql
- Can confirm this via /etc/my.cnf

```
# cd /mnt/img/etc
# cat my.cnf
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
…
```

Step 1b: Grab the datadir



Step 2: Prepping Data for Use

```
# /etc/init.d/mysqld stop          stops current DB instance
Stopping MySQL…
# cd /var/lib
# mv mysql mysql.orig              put current MySQL dir out of the way
# tar zxf /root/mysql.tgz          unpack extracted MySQL dir
# chown -R mysql:mysql mysql       "mysql" user may have different UID
```

Step 3: Database Access

- You've just copied an entire MySQL installation
- Which contains DB access passwords
- Passwords that you may not know…

- Trick: restart MySQL w/ --skip-grant-tables opt:

```
# mysqld_safe --skip-grant-tables &
[1] 19448
# mysql -u root
…
mysql>
```

Step 4a: Databases? What Databases?

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| bot                |
| mulesrus           |
| mysql              |
| postfix            |
+--------------------+
5 rows in set (0.00 sec)

mysql> use postfix;
Database changed
```

Step 4b: Tables? What Tables?

```
mysql> show tables;
+------------------------+
| Tables_in_postfix      |
+------------------------+
| admin                  |
| alias                  |
| alias_domain           |
| config                 |
| domain                 |
| domain_admins          |
| fetchmail              |
| log                    |
…
+------------------------+
13 rows in set (0.00 sec)
```

Step 4c: Count Before Dumping

```
mysql> select count(*) from admin;
+----------+
| count(*) |
+----------+
|        3 |
+----------+
1 row in set (0.00 sec)

mysql> select * from admin;
+---------------------+-----------------------+-----------…
| username            | password              | created
+---------------------+-----------------------+-----------…
| inga@sysiphus.com   | N8styB0yz             | 2010-10-11…
| jerry@sysiphus.com  | Jerry'sScriptKiddies  | 2010-10-13…
| ashley@sysiphus.com | GoneWithTheWinds      | 2010-10-13…
+---------------------+-----------------------+-----------…
3 rows in set (0.00 sec)
```

Step 4c: Sampling

```
mysql> select count(*) from mailbox;
+----------+
| count(*) |
+----------+
|     4368 |
+----------+
1 row in set (0.00 sec)

mysql> select * from mailbox limit 3;
+---------------------+-----------------------+-----------…
| username            | password              | name      …
+---------------------+-----------------------+-----------…
| jerry@mulesrus.com  | Jerry'sScriptKiddies | Jerry Roge…
| inga@mulesrus.com   | N8styB0yz             | Inga N Gut…
| ali@mulesrus.com    | 123password           | Ali Willia…
+---------------------+-----------------------+-----------…
3 rows in set (0.00 sec)
```

Step 4c: More Sampling

```
mysql> select distinct domain from mailbox;
+-----------------+
| domain          |
+-----------------+
| MulesRUS.com    |
| ShipMyStuff.com |
+-----------------+
2 rows in set (0.00 sec)

mysql> select * from mailbox
    -> where domain = 'ShipMyStuff.com' limit 3;
+-----------------------+----------------+--------------+…
| username              | password       | name         |…
+-----------------------+----------------+--------------+…
| aj@shipmystuff.com    | keepontruckin' | Alex Johnson |…
| cbrown@shipmystuff.com | SmokinAgain    | Carson Brown |…
| chase@shipmystuff.com  | PaperChase…
```

Step 4c: Choosing Columns

```
mysql> describe admin;
+----------+--------------+------+-----+-----------------…
| Field    | Type         | Null | Key | Default         …
+----------+--------------+------+-----+-----------------…
| username | varchar(255) | NO   | PRI |                 …
| password | varchar(255) | NO   |     |                 …
| created  | datetime     | NO   |     | 0000-00-00      …
| modified | datetime     | NO   |     | 0000-00-00      …
| active   | tinyint(1)   | NO   |     | 1               …
+----------+--------------+------+-----+-----------------…
5 rows in set (0.00 sec)

mysql> select username, password, created from admin;
+-------------------+---------------+-------------------+
| username          | password      | created           |
+-------------------+---------------+-------------------+
| inga@sysiphus.com | …
```

Step 5a: Create Output Dir

- MySQL can write data to files
- Output dir must be writable by "mysql" user:

```
# mkdir /tmp/mysql-data
# chown -R mysql:mysql /tmp/mysql-data
# chmod 700 /tmp/mysql-data
```

Step 5b: Tab-Delimited or CSV?

```
mysql> select *
    ->    into outfile '/tmp/mysql-data/mailbox.tab'
    -> from mailbox;
Query OK, 4368 rows affected (0.00 sec)

mysql> select *
    ->    into outfile '/tmp/mysql-data/admin.csv'
    ->    fields terminated by ','
    ->    optionally enclosed by '"'
    ->    lines terminated by '\r\n'
    -> from admin;
Query OK, 3 rows affected (0.00 sec)
```

Step 5b: Command-Line Version

- Comes with MySQL installation

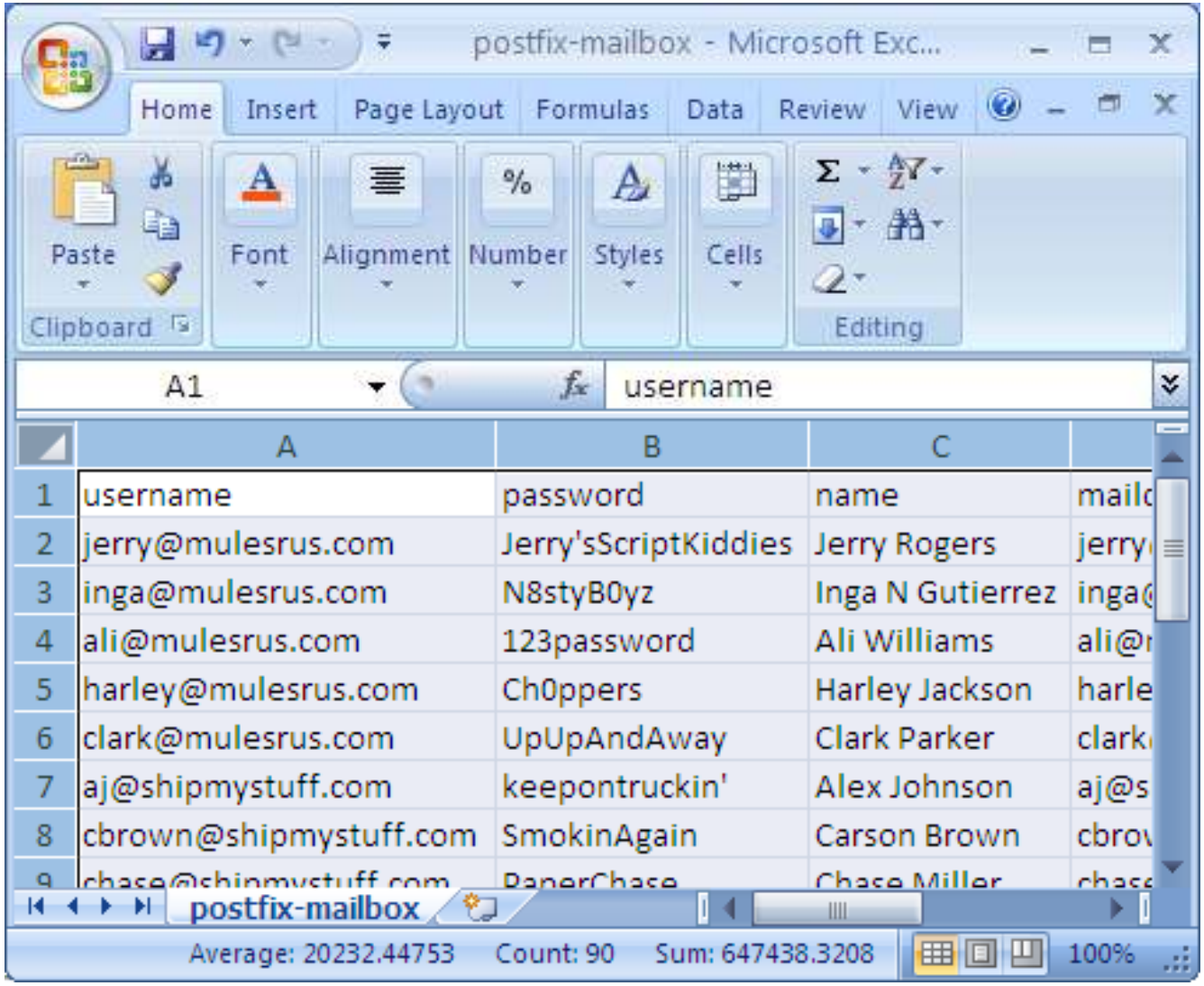
```
# mysqldump -T /tmp/mysql-data
    --fields-terminated-by=,
    --fields-enclosed-by='"'
    --lines-terminated-by='\r\n'
    -u root postfix
```

- Tool I developed to simplify things:

```
# mysql2csv
```

dumps all dbs to current directory

Which Finally Gets Us To…



Wrapping Up

- Any final questions?
- Thanks for listening!

hal@deer-run.com

http://www.deer-run.com/~hal/mysql2csv