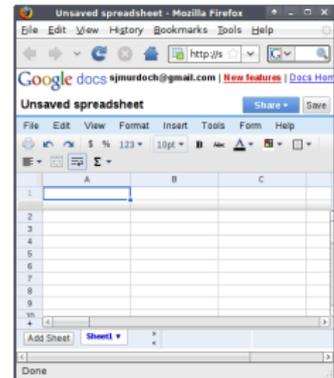




# Evidence in fraud cases is increasingly complex and voluminous

- Modern technology increases both the complexity and quantity of evidence in fraud cases
- This offers both challenges and opportunities to investigators
- Criminals may also exploit this complexity in order to frustrate investigation
- In this talk I will discuss two particular examples
  - Cloud computing
  - Chip & PIN
- The general principles will also be applicable to other areas

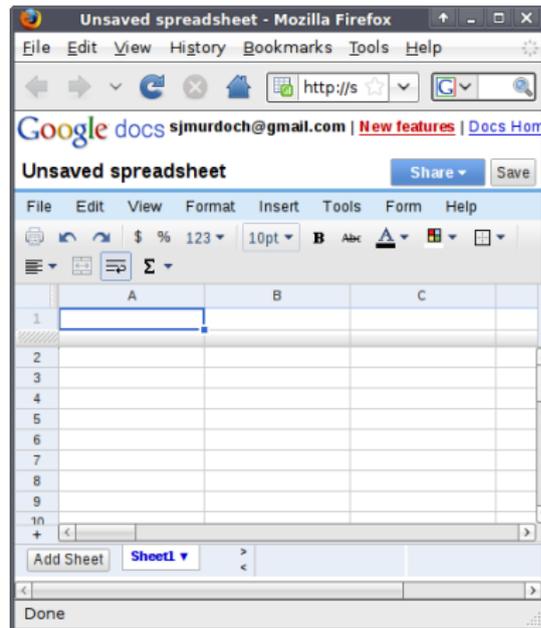
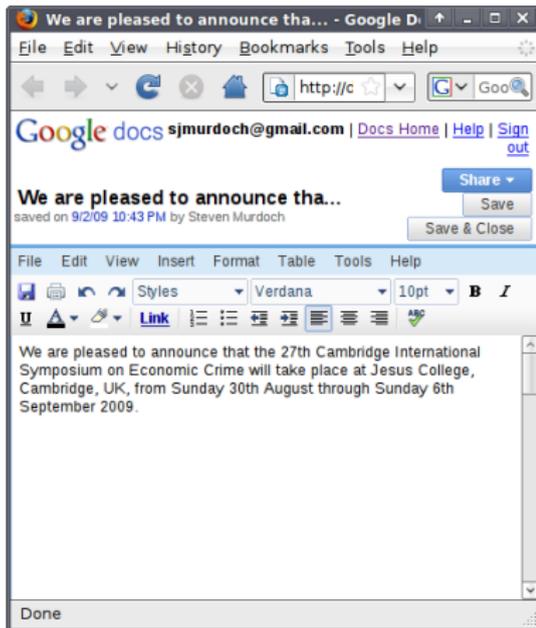


## Cloud computing is not new



In the early days of computers, people rented computer time on mainframes because computers were too expensive to buy

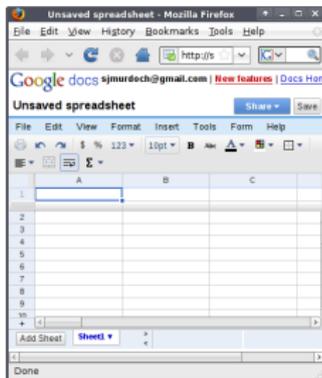
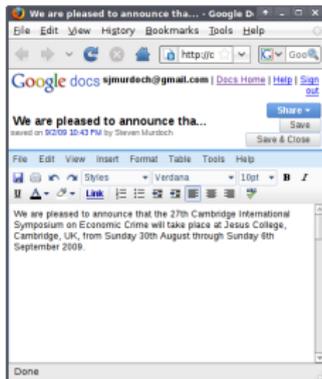
# Cloud computing is not new



Now people rent time on computers because computers are so cheap it is not worth maintaining them

# Cloud computing does change things

- Data is stored in computers owned by people other than the suspect
- These computers may be in different countries
- They probably need a password to access them
- It may not be as easy to perform searches
- Even finding out which ones exist is difficult
- Establishing a chain of custody can be difficult



## Imagine you are an investigator

- You seize computers belonging to a suspect
- You find no documents, but Google Docs in the history
- Suppose you have the password; can you log into Google's US-based servers to read the documents?
- Suppose you don't have the password; can you demand the suspect hand it over?
- Suppose you don't find the password; could you hack into the Google server to read these documents?

**Where does Mutual Legal Assistance need to come in?**

**When would you like it to?**

# Chip & PIN is now being deployed worldwide

- Chip & PIN, based on the EMV (EuroPay, Mastercard, Visa) standard, is deployed throughout most of Europe
- The UK was an early adopter (started 2003, complete by 2006)
- Deployment has started in Canada and Mexico
- Transactions (point-of-sale and ATM) are authorized using a smart card and PIN
- Fraud levels dipped in 2005–2006, but criminals adapted (£610m in 2008)

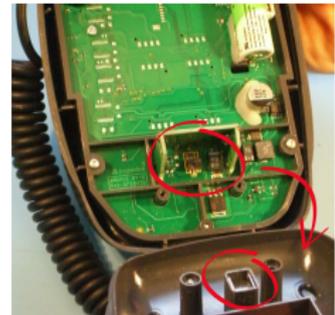


Chip and PIN



# Chip & PIN changed fraud

- Criminals shifted to other areas (notably card-not-present)
- Vulnerabilities in the Chip & PIN system itself were also exploited
- Could be used for third-party fraud, and also indirectly for first-party fraud
- Establishing what has happened depends on the evidence, and there is a lot more with Chip & PIN (and it is more complex)
- Most relevant evidence is now held by the bank, as is the necessary information to interpret it
- Causes a problem if the bank isn't interested in co-operating



## Not all bad news either

- Chip & PIN transactions create a cryptographic audit trail which can be verified by a third party: Good for investigating alleged insider fraud
- Cards maintain a log of the number of transactions they have completed, and often other information too: Good for investigating alleged first-party fraud
- While various types of fraud can happen, often there is forensic evidence in log files, e.g.
  - By tampering with the communication between the card and terminal, a criminal can use a card without knowing the correct PIN
  - However comparing the card's transaction summary to the receipts and merchant log will show what has happened



BRANCH		
BETWEEN 00.00 & 24.00		
2006 - 28th February 2006		
TYPE	(Transaction date: 22	
xxx		
- HBS BALANCE ENQUIRY		
04041687	19010200	00000000
* 00000010	49175401	68719010
* 01841706	02220602	22060222
* 40404040	40404040	40404040
* F8F0F4D9	C5C1C4D5	C740E6C8
* 40404040	4040F0F0	F0F5F4F7

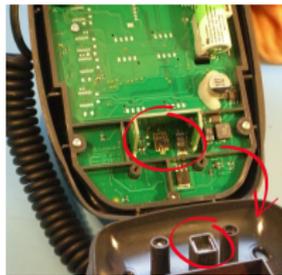
# Still, it is hard to investigate

- I've worked in the investigation of several Chip & PIN fraud cases, as a formal expert witness or just assisting the police or customer
- There is often a long time between fraud being reported and investigated
- In the intervening time, banks may delete the evidence, even for transactions under dispute
- Banks are reluctant to disclose how their systems work, or what evidence means
- Standard procedure is that once a card is suspected to have been used in fraud, it should be destroyed
  - I have only succeeded collecting evidence in one out of five cases, and that was because the customer refused to follow bank instructions

```
Trying PROTOCOL_MVY
PIN: > Reading master file
- Reading file IPAY.SYS.D0F1
sending command: 00a40400e315041592e5359532e4444630310
got RESPONSE: 6126
sending command: 00C00000026
got RESPONSE: 6F2F840E315041592E5359532E444463031A51280
0101BF0C0CC50AFFFF3F00000002FFFF029000
TLV: 6F2F840E315041592E5359532E444463031A512800101BF0C
CC50AFFFF3F0000002FFFF029000
$$ File Control Information (FCI) Template (6F):
  $$ Dedicated File (DF) Name (84):
    315041592E5359532E444463031 - 1 P A Y . S Y S .
D D F 0 1
  $$ FCI Proprietary Template (A5):
  $$ Short File Identifier (SFI) (8B):
    01 - ...
  $$ FCI Issuer Discretionary Data (BF0C):
  $$ Unknown (CS):
    FFFF3F0000002FFFF02 - .....7 .....
...
SFI: 01
- Reading SFI record
sending command: 00b2010c00
got RESPONSE: 6C22
sending command: 00b2010c22
got RESPONSE: 7020611E4F07A00000000410105010406173746572
4361726420202020208701019000
TLV: 7020611E4F07A00000000410105010406173746572436172642
02020202020208701019000
$$ Application Elementary File (AEF) Data Template (70):
  $$ Application Template (61):
  $$ Application Identifier (AID) (4F):
    A0000000041010 - .....
  $$ Application Label (50):
    40617374657243617264202020202020 - M a s t e
r c a r d .....
  $$ Application Priority Indicator (87):
    01 - ...
AID: A000000041010
- Reading AID record
sending command: 00a4040007A000000004101000
got RESPONSE: 6121
sending command: 00C00000031
got RESPONSE: 6F2F8407A0000000041010A5245010406173746572
436172642020202020870101BF0C0C50A01017F514700030FFF03
9000
TLV: 6F2F8407A0000000041010A5245010406173746572436172642
020202020870101BF0C0C50A01017F514700030FFF039000
$$ File Control Information (FCI) Template (6F):
  $$ Dedicated File (DF) Name (84):
    A0000000041010 - .....
  $$ FCI Proprietary Template (A5):
  $$ Application Label (50):
    40617374657243617264202020202020 - M a s t e
r c a r d .....
  $$ Application Priority Indicator (87):
    01 - ...
  $$ FCI Issuer Discretionary Data (BF0C):
  $$ Unknown (CS):
    01017F514700030FFF03 - .....Q G .....
...
> Reading records
- Get processing options
```

# Conclusions

- Evidence will continue to grow in terms of complexity and volume
- Procedures in fraud investigation will need to change to adapt
- Cloud computing brings challenges, most notably the cross-border nature
- Chip & PIN offers new evidence, but obtaining and interpreting this is difficult
- I have an article explaining Chip & PIN security, evidence, and forensics in the upcoming *Digital Evidence and Electronic Signature Law Review*



SEARCH		
BETWEEN 00.00 & 24.00		
2006 - 28th February 2006		
TYPE	(Transaction date: 22	
XXXX		
	= HBS BALANCE ENQUIRY	
04041687	19010200	0000000C
00000010	49175401	68719010
01841706	02220602	22060222
40404040	40404040	40404040
F8F0F409	C5C1C4D5	C740E6C8
40404040	4040F0F0	F0F5F4F7

