Evidence in Fraud Cases
Complexity and Access

Steven J. Murdoch
http://www.cl.cam.ac.uk/users/sjm217/

UNIVERSITY OF
CAMBRIDGE
Computer Laboratory

www.torproject.org

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 & 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
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
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*