

## Digital Forensics Investigations of Social Networks: Learning from other Disciplines

**Dr John Haggerty**

J.Haggerty@salford.ac.uk

<http://www.cse.salford.ac.uk/profiles/haggerty/>

---

---

---

---

---

---

---

---

### Presentation outline

- Digital forensics background
- Social networks
- Investigating SNS
- Investigating email
- Learning from other disciplines
- Challenges to SNA

---

---

---

---

---

---

---

---

### Digital forensics – a definition(?)

- “*Digital forensics: the study of how people use computers to inflict mischief, hurt and even destruction*” (Mohay et al, 2003)
- “*The application of computer investigation and analysis techniques to determine potential evidence*” (Lin & Seberry, 2003)
- No accepted definition
  - However, generally focuses on investigation and analysis to determine culpability

---

---

---

---

---

---

---

---

## Digital forensics today

- Wide range of digital forensics activities and tools being used today, e.g.
  - Law enforcement
  - Data recovery
  - Audit
  - Security
- Increasingly being deployed in organisations
  - Without the robustness of law enforcement processes?

---

---

---

---

---

---

---

---

## Digital forensics tomorrow

- The digital landscape has changed
  - Pervasiveness of computing devices
  - No longer just one suspect/one computer
- Need to move beyond law enforcement “evidence extraction” legacy
  - In research, beyond the “what are the computer forensics artefacts of...” in publications
- New tools and techniques required

---

---

---

---

---

---

---

---

## Social networks

- Social networks form a major part of **today's** and the **future** digital landscape
- What is a social network?
  - “A social network consists of a finite set or sets of **actors** and the **relation or relations** defined upon them. The presence of **relational information is a critical and defining feature** of a social network.”  
(Wasserman & Faust, 1994) [my emphasis]

---

---

---

---

---

---

---

---

## Social networks in digital form

- Social network digital representations are manifested in various forms e.g.
  - Email
  - Social network sites
  - Mobile phones
  - Virtual worlds
  - Content sharing sites
- Social network analysis (SNA) is/will be a major focus of digital forensics

---

---

---

---

---

---

---

---

## Social networks - usage

### Top Eight Web Sites Worldwide, Ranked by Page Views, September 2007 (billions)

|             |       |
|-------------|-------|
| 1. Yahoo!   | 55.31 |
| 2. MySpace  | 49.72 |
| 3. Google   | 34.63 |
| 4. Facebook | 34.54 |
| 5. Orkut    | 32.80 |
| 6. Live.com | 31.90 |
| 7. MSN      | 29.52 |
| 8. YouTube  | 21.37 |

Note: ages 15+; home and work locations; excludes traffic from public computers such as those at Internet cafés or access from mobile phones or PDAs  
Source: comScore World Metrix as cited by The Wall Street Journal, October 19, 2007

Image source: <http://michaekorey.nirety.com/blog/tabid/51101/bid/9760/Should-CEO-s-use-Facebook-Twitter.aspx>

---

---

---

---

---

---

---

---

## Social networks - facebook

- Some statistics from facebook:
  - >350 million active users
  - >50% active users log in on any given day
  - >3.5 billion pieces of content shared each week (photos, notes, news stories, etc.)
  - >2.5 billion photos uploaded each month
  - Average user has 130 friends and spends 55 minutes per day on the site
  - Average user writes 25 comments on content each month

Source: <http://www.facebook.com/press/info.php?statistics>

---

---

---

---

---

---

---

---

## Inter-disciplinarity of SNA

- SNA is not unique to digital forensics
  - Humanities, e.g. History
  - Social Sciences, e.g. Sociology
  - Sciences, e.g. Psychology
- These other disciplines have their own frameworks, methodologies, etc. for SNA
  - Can we learn from these disciplines?
- Digital forensics ideally suited as it is inter-disciplinary in nature

---

---

---

---

---

---

---

---

## Social network characteristics

- Social Network Services are not social networks (Ackland, 2009)
  - Means by which social networks may be manifested
- Social network relationships are not equal
  - ‘Weak’ versus ‘strong’ ties (Granovetter, 1973)
- Relationships can be assessed/measured
  - Centrality (Freeman, 1978/79)

---

---

---

---

---

---

---

---

## Social network characteristics

- Continued associations – relationships as defining features
  - ‘Relational cohesion’ (Lawler & Yoon, 1996)
- People invest in social networks
  - Social capital (Portes, 1998)
  - Business (Haggerty & Haggerty, 2010)
- Create perceptions of self and other
  - Perceptions of SN relationships in children (Furman & Burmester, 1985)

---

---

---

---

---

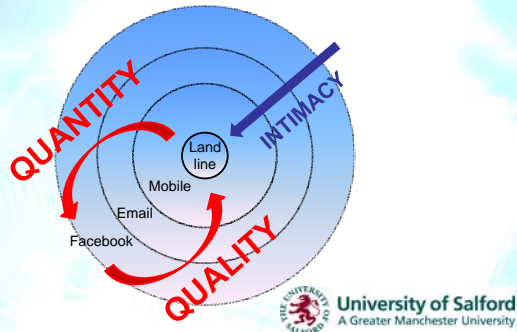
---

---

---

## SNS and relationships

- Degrees of intimacy reflected in SNS?



---

---

---

---

---

---

---

---

## EET overview

- Email Extraction Tool for initial analysis
  - Haggerty, Lamb & Taylor (2009)
- First line analysis of 'tangible' versus 'intangible' evidence
- Recognises that folder use will give rudimentary indication of social networks
- Of interest
  - Key actors, organisation of networks, power relationships, etc.

---

---

---

---

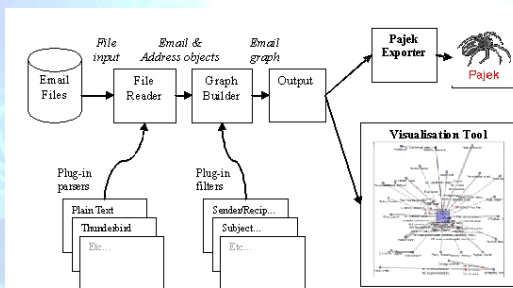
---

---

---

---

## EET overview



---

---

---

---

---

---

---

---

## EET background

- Identify social patterns from email data
  - FROM, TO, CC and SUBJECT
  - Forwarded emails (the 'hidden' email problem)
  - Provides different viewpoints of the network
  - Integrated workspace
- Prototype developed for analysis of Mozilla Thunderbird format

---

---

---

---

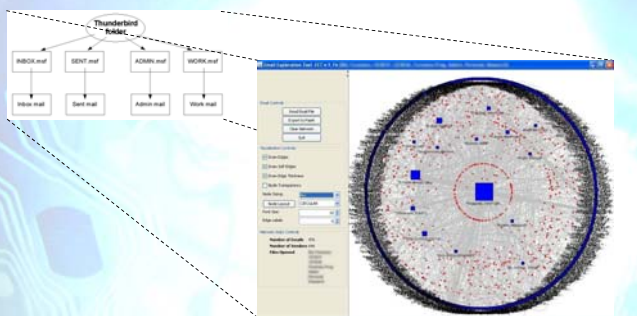
---

---

---

---

## EET overview



---

---

---

---

---

---

---

---

## Learning from other disciplines

- Networks are complex
  - Therefore require complexity in their analysis
- Networks change over time
  - Provide actors different opportunities to access social, human, economic, etc. capital
- Networks are social, political and cultural constructs
  - Need to understand them in these terms

---

---

---

---

---

---

---

---

## Learning from other disciplines

- Networks can be measured and analysed
  - Different measures provide different viewpoints for the analysis
- SNS are not social networks
  - They provide access to social networking opportunities (but there can be a lot of redundancy)
- Social networks can work for or against the actors involved

---

---

---

---

---

---

---

---

## Challenges to SNA

- Challenges exist to SNA across disciplines
  - Intangible vs. tangible evidence
    - Quantifying the unquantifiable
  - Volume of data to be examined
    - Process automation
  - The 'ego'-centricity problem
    - "significant evidence is not evidence of significance" (Milne, 2000)
  - Mitigating missing data
    - Data modelling

---

---

---

---

---

---

---

---

## Challenges to SNA

- Robustness of results
  - Interpretation or substantiated opinion
- Qualitative vs. quantitative analysis
  - Deeper understanding or generic trends
- Geo-political constraints
  - Access to suspects
- Change over time
  - Deeper understanding of events
- Meaningful representation of data
  - Computer to provide different analysis viewpoints

---

---

---

---

---

---

---

---

## Summary

- Social networks form a major part of today's and the future digital landscape
- SNS are the means by which social networks are manifested in digital form
- Investigation of social network data is extremely complex
- Many challenges remain in digital forensics investigations using SNA

---

---

---

---

---

---

---

---