Pervasive Social Networking Forensics: Intelligence and Evidence from Mobile Device Extracts

Seoultech

Tumenbayar

2017/11/20

Abstract

- In pervasive social networking forensics, mobile devices (e.g. mobile phones) are a typical source of evidence.
- There is an ongoing and increasing growth in the volume of data available for evidence and intelligence analysis.
- Potential for information relevant to a range of crimes within the extracted data.
- As terrorism and organised crime investigations, with potential cross-device and cross-case linkages.

1.Introduction

- Social networking services for both individual (e.g. Facebook and LinkedIn) and enterprises (e.g. Yammer) are increasingly popular.
- Mobile devices are increasingly the focus of criminal investigations.
- such as those used by organised crime and terrorist groups.
- This growth has contributed to an increase in the volume of digital forensic data.
- Mobile device forensics is a relatively new field of digital forensics.
- Whilst processes to extract data are addressed by commercial offerings.

1.Introduction

- such as MSAB XRY, Cellebrite UFED, and Oxygen Forensic Suite.
- the various tools output the extracted data in differing formats.

- Across a criminal or civil investigation, there may be a variety of devices to be examined, and the use of a multiple tools, methods, and processes may be required to extract and analyse data.
- Evidence from the investigation of social networking services (e.g. social networking apps) can include call and contact information to show relationships.
- SMS and MMS messages to substantiate communication and picture and video data to show evidence of crimes or other breaches of legislation or policy.

1.Introduction

- Current commercial forensic solutions extract available data, and allow for exports and reports to be produced from the data.
- The extracted data, exported files, and reports, are growing in volume, influenced by the growing storage volume, growing data type, and number of devices – the 'big forensic data' challenge.
- In this paper, investigate the growth in mobile device forensics and a process of digital forensic intelligence analysis across a variety of devices.
- apply the process to test data using a range of mobile forensic commercial software.

2. Background

2.1 South Australia Police - Electronic Evidence 2000-2015

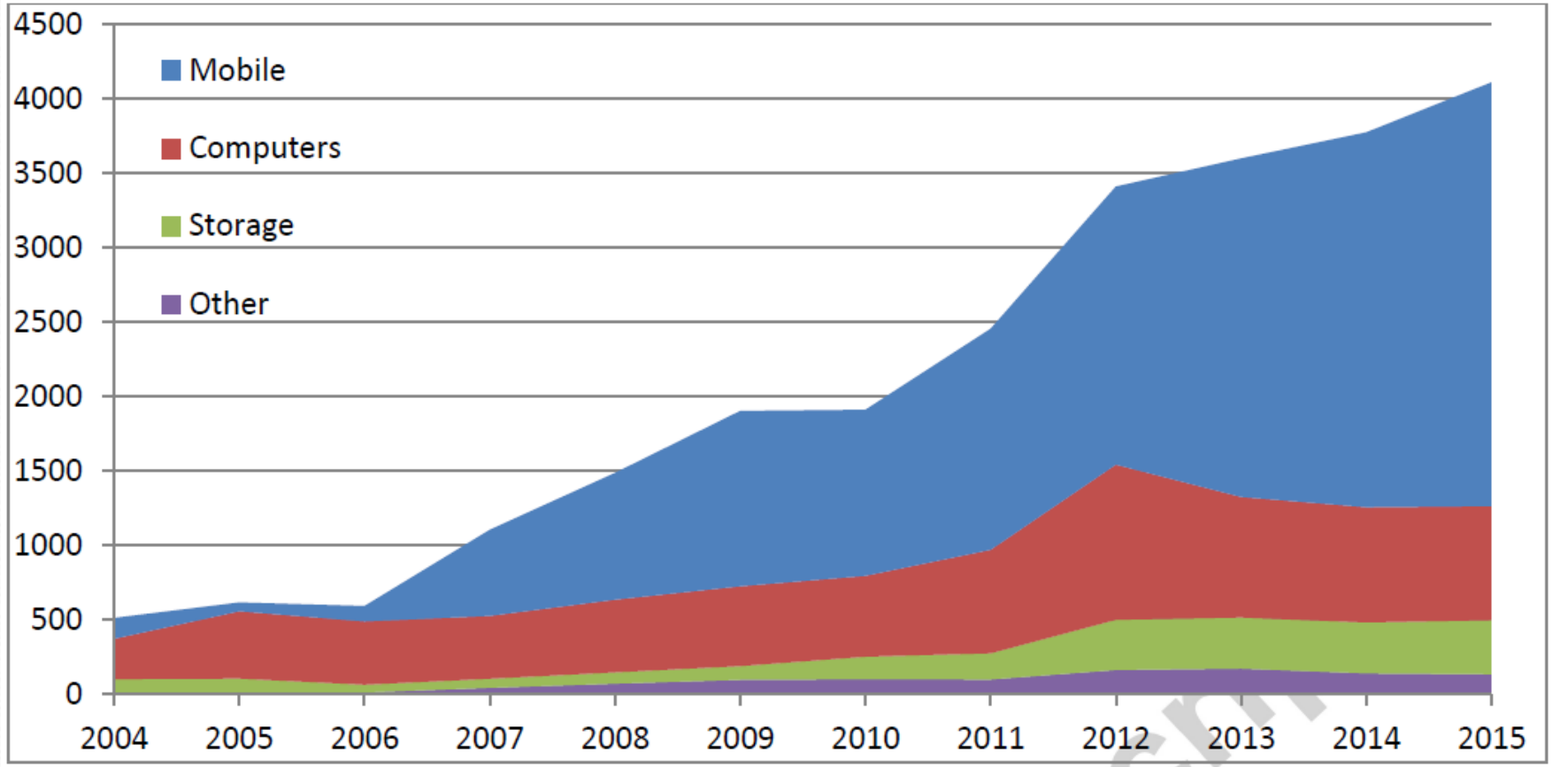
- In 2009, Turnbull et al examined data from South Australia Police (SAPOL) Electronic Crime Section (ECS) which showed a growth in requests for analysis of electronic evidence.
- The data per financial year (01 July to 30 June) has been divided into categories :
  - Mobile phones
  - Computers
  - Storage
  - Others

Devices presented for analysis per year (2000-2015) (SAPOL ECS) FY

FY	Total Cases	Mobile Phones	Computers	Storage	Others	Total Devices
2000	**40**					**48**
2001	**140**					**226**
2002	**175**					**301**
2003	**197**					**341**
2004	**269**	140	271	87	15	**513**
2005	**273**	59	452	93	13	**617**
2006	**268**	103	425	52	13	**593**
2007	**402**	578	422	61	44	**1105**
2008	**548**	851	488	76	72	**1487**
2009	**661**	1177	536	92	98	**1903**
2010	**700**	1115	543	151	102	**1911**
2011	**872**	1484	695	176	100	**2455**
2012	**1014**	1867	1042	337	164	**3410**
2013	**1203**	2273	810	343	173	**3599**
2014	**1226**	2517	774	342	341	**3774**
2015	**1417**	2846	766	363	135	**4110**
Total	**9405**	15013	7226	2173	1070	**26393**

2. Background

The data is charted visually highlights the growth in mobile devices presented for analysis since 2006.



2. Background

2.2 FBI Regional Computer Forensic Labs 2006-2013

- To determine if the growth observed in the SAPOL ECS data is reflected in other jurisdictions
- The data in the Federal Bureau of Investigation (FBI) Regional Computer Forensic Labs (RCFL) Financial Year Annual Reports.

2. Background

Mobile Telephone examinations per Year (FBI RCFL)

Annual Report	Mobile Phones	Comment
2006	701	Examinations
2007	1486	Examinations
2008	2226	Examinations
2009	1953	CPIK process introduced
2010	1909	Examinations
2011	6870	CPIK and VCPK
2012	9891	CPIK and VCPK
2013	11362	CPIK and VCPK

Cellular telephone kiosk (CPIK)

Virtual Cell Phone Kiosk (VCPK).

Regional Computer Forensic Labs (RCFL)

- In 2009 Annual report , a Self-service process was introduced.
- (CPIK) resulting in the RCFL mobile phone examinations dropping from previous years.
- Than CPIK examination is listed in 2011 , 2012 and 2013 Annual reports.

2. Background

2.3 Mobile Phone and Portable Storage Growth 2003-2015

Year	Apple iPhone		Apple iPad		Samsung Galaxy		MicroSD	SD Card	Price per GB
2003								1GB	$330
2004								2GB	$120
2005							512MB		
2006							2GB	4GB	$55
2007	3G	16GB					8GB	8GB	$22.50
2008							16GB	32GB	$10.94
2009	3GS	32GB			i7500	8GB			
2010	4	32GB	iPad	64GB	S	16GB	32GB	64GB	$5.47
2011	4S	64GB	2	64GB	S2	32GB	64GB	128GB	$3.13
2012	5	64GB	Retina	64GB	S3	64GB		256GB	$3.52
2013	5S	64GB	Air	128GB	S4	64GB			
2014	6	128GB	Air2	128GB	S5	64GB	128GB	512GB	$1.56
2015	6S	128GB	Pro	256GB	S6	128GB	200GB		

2. Background

2.4 Digital Forensic Intelligence Analysis

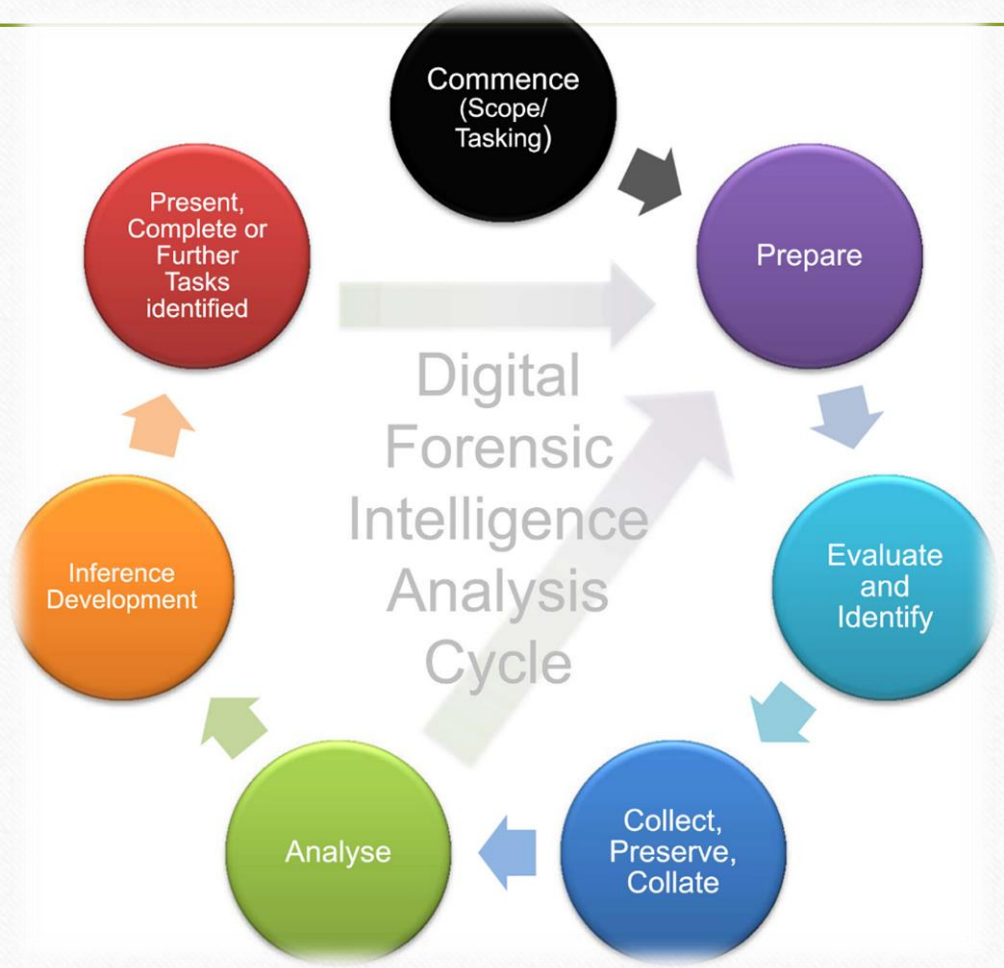
- Forensic Intelligence is; “the accurate, timely and useful product of logically processing (analysis of) forensic case data (information) for investigation and/or intelligence purposes”.
- Criminal intelligence analysis methodologies, such as those outlined in the United Nations Office on Drugs and Crime Criminal Intelligence Manual for Analysts, include link charts, timeline analysis, data correlation, and other analysis methods.

3.Digital Forensic Intelligence Analysis of Mobile Phones

- Digital Forensic Intelligence Analysis is a process of applying Criminal Intelligence Analysis methodologies to Digital Forensic data.
- The steps from the Intelligence Analysis Cycle and the Digital Forensic Analysis Cycle to form the Digital Forensic Intelligence Analysis Cycle (DFIAC).

3.Digital Forensic Intelligence Analysis of Mobile Phones

Proposed Digital Forensic Intelligence Analysis Cycle



- In this process, both the Intelligence Analysis Cycle, and the process of Digital Forensic Analysis are cyclical,
- it is an organic cycle during which analysts may uncover information relating to another mobile device,

and return to a process of preparation, evaluation, identification, collection, preservation, and collation for the new device and its data.

3.Digital Forensic Intelligence Analysis of Mobile Phones

3.1 Mobile Device Forensic Extracts

- In the field of mobile device forensics, there are a number of commercial solutions to extract
- Analyse data, such as; MSAB XRY, Cellebrite UFED, Radio Tactics ACESO, Access Data MPE+, Paraben Forensic, Oxygen Forensic, and CellXtract.
- This highlights that in a criminal or civil investigation, where multiple devices are crucial to a case
- Differing tools and methods may be needed to extract and analyse data from a variety of devices.

3.Digital Forensic Intelligence Analysis of Mobile Phones

3.2 Digital Forensic Mobile Phone Extracts

- This research examines the data output type from a variety of tools to determine opportunities for intelligence analysis processes to be applied.
- Focus on the data export formats available across the various tools.
- The software utilised included:

- MSAB (formerly Micro Systemation AB) XRY
- Cellebrite UFED
- Oxygen Forensic
- Guidance Software EnCase
- Paraben Forensic
- and Magnet Forensic IEF.

3.Digital Forensic Intelligence Analysis of Mobile Phones

3.2 Digital Forensic Mobile Phone Extracts

- Each tool was used to access a range of test data extracts.
- Then export data in the various options available for each tool.
- The test data used for the research included :
  - Mobile phone test data extracts from the Digital Forensic Corpus.
  - Data extracts available from the Oxygen Forensic website.
  - Data extracted as part of our previous cloud storage research.
- This research focuses on methods to reduce large volumes of disparate extracted data.
- Methods to export data to a common format.

4.Mobile Phone Extracts

- Research focus on the export potential of the various software tools.
- is not intended to be a comparison of the capability of each tool.
- The data output potential of each of the mobile phone forensic tools we used test data available for each tool
- These contained a wide variety of data, rather than using a limited number of available mobile phones and extracting the same data using a variety of tools

4.Mobile Phone Extracts

- Researcher aiming for a wide variety of disparate data in the extracts.
- This section outlines the data exports available for each of the tools examined :
  - MSAB XRY
  - Oxygen Forensic Suite
  - Cellebrite UFED
  - EnCase 7
  - Paraben
  - Magnet Forensic Internet Evidence Finder.

4.Mobile Phone Extracts

4.1 MSAB XRY 6.12.1

- For this research, examine the process of exporting data using test data files from previous research.
- These consisted of a range of extracts from a 16GB Apple iPhone 3G which were undertaken using MSAB XRY 6.3, each resulting in average of 12.8GB per XRY file.
- The available export formats from XRY include:

- PDF
- DOCX
- XLSX, and XML formats.

4.Mobile Phone Extracts

4.1 MSAB XRY 6.12.1

- Each test file was opened and the data was exported using the options available in XRY 6.12.1.
- The exported XLSX reports comprised the extracted and parsed information from a range of data sources including :

- Contacts,
- Calls,
- Messages,
- Chat, and other Application data.

Format	Size(MB)
PDF	40
DOCX	117
XLSX	768(kB)
XML	20

- The exported files included pictures and videos which may be relevant in some cases.

4.Mobile Phone Extracts

4.2 Oxygen Forensic Suite 6.4.0.67

- A variety of mobile device extracts are available from the Oxygen website in the Oxygen OFB format.
- These are compressed in a Zip container format, and can be expanded using unzip software.
- The original size of the devices is not listed in the extract or on the website, and a comparison could not be made to the original size of the device.
- Each test file was opened and the data was exported in the various options using Oxygen Forensic Suite 2014 version.

4.Mobile Phone Extracts

4.2 Oxygen Forensic Suite 6.4.0.67

- Each test file was opened and the data was exported in the various options using Oxygen Forensic Suite 2014 version.

- Extracted data in the XLS spreadsheets included :

  - Browser Activity
  - Map information, iOS call logs,
  - Email, SMS and MMS messages,
  - Instagram, KiK, and Parsed Search Queries.

Format	Size
PDF	31(MB)
RTF	11(MB)
XLS	3.6(MB)
XML	2.6(MB)

4.Mobile Phone Extracts

Cellebrite UFED 3.9.2.4

- The Digital Forensic Corpus includes a number of extracts which appear to be from a Samsung GSM-I9020a Nexus S obtained using Cellebrite UFED 1.1.9.4 in July 2012.
- The extracts are available in zip format, and unzip to the full UFED binary file extracts.
- Exported to available report formats, including :
  - PDF, DOCX, XLSX, and XML.

Format	Size
PDF	12(MB)
DOCX	247(kB)
XLSX	218(kB)
XML	1(MB)

4.Mobile Phone Extracts

4.4 Guidance Software EnCase 7.09.04

- Included in the Digital Forensic Corpus are file extracts from an Apple iPhone which appear to be from EnCase forensic software, saved in a logical container (L01) format.
- Each test file was opened and the data was exported in the various options using EnCase.
- The five test data files comprising 92.7MB in L01 files.
- The Spreadsheet (CSV) files were the smallest Format which included :
  - Contacts, calls,
  - Message and Application information.

Format	Size(MB)
PDF	14.7
TXT	21(kB)
RTF	5.3
CSV	8.5(kB)
XML	32.8(kB)

4.Mobile Phone Extracts

4.5 Paraben Device Seizure 6.66

- Paraben Device Seizure 6.66 was used with extract files from an iPhone and from an Android phone, in Paraben DS format totalling 1.6GB.
- Each test file was opened and the data was exported in the 14 various options using Paraben 6.66 Software.
- The XLS files were the smallest format which included :

  - Contacts, calls, message

  - Web bookmarks, and application information

    such as Kik and TextFree.

Format	Size(MB)
PDF	3.67
TXT	6.9
HTML	253.8
CSV	14.2
XML	1.2

4.Mobile Phone Extracts

4.6 Internet Evidence Finder (IEF) 6.4.2.0070

- In the Digital Forensic Corpus, there are mobile device extract files in the E01 format, which appear to be AccessData MPE+ extracts.
- These files were viewed using FTK Imager 3.2.0.0, and the data within each container was extracted.
- The E01 files were then examined using Magnet Forensics Internet Evidence Finder and report outputs produced.
- The CSV files were the smallest format which included :

- Contacts, calls, messages, emails, Gmail

- Web bookmarks, and other application information.

Format	Size(MB)
PDF	58.9
HTML	157
CSV	1.76
XLS	120
XML	13.9

4.Mobile Phone Extracts

4.7 Summary of Mobile Phone Exports

- The various options to export data in a variety of formats from :
  - EnCase, FTK Imager, Cellebrite UFED
  - MSAB XRY, IEF, Oxygen, and Paraben.
- The data volumes from each tool used to process the test data, and the totals across the devices.
- A volume reduction from a total of 339.9 GB to 207.6 MB in spreadsheets (CSV, XLS, or XLSX), and 485.4 MB for XML files,
- The exported and parsed data including contacts, calls, messages, emails, Gmail, web bookmarks, GPS coordinates, and a range of other application information.

4.Mobile Phone Extracts

4.7 Summary of Mobile Phone Exports

Total data volume for the exported Test data

	Source / Files (GB)	Container size (GB)	XLS or CSV (MB)	XML (MB)
MSAB XRY	128	99.4	6.062	162.5
Oxygen	4.8	3.7	129.3	39.1
Cellebrite	1.076	1.082	1.307	6.259
Encase 7	0.0857	0.082	42.5	164.2
Paraben	2.92	0.092	14.4	2.36
IEF	203	1.684	14	111
Total	339.9 GB	109.2 GB	207.6 MB	485.4 MB

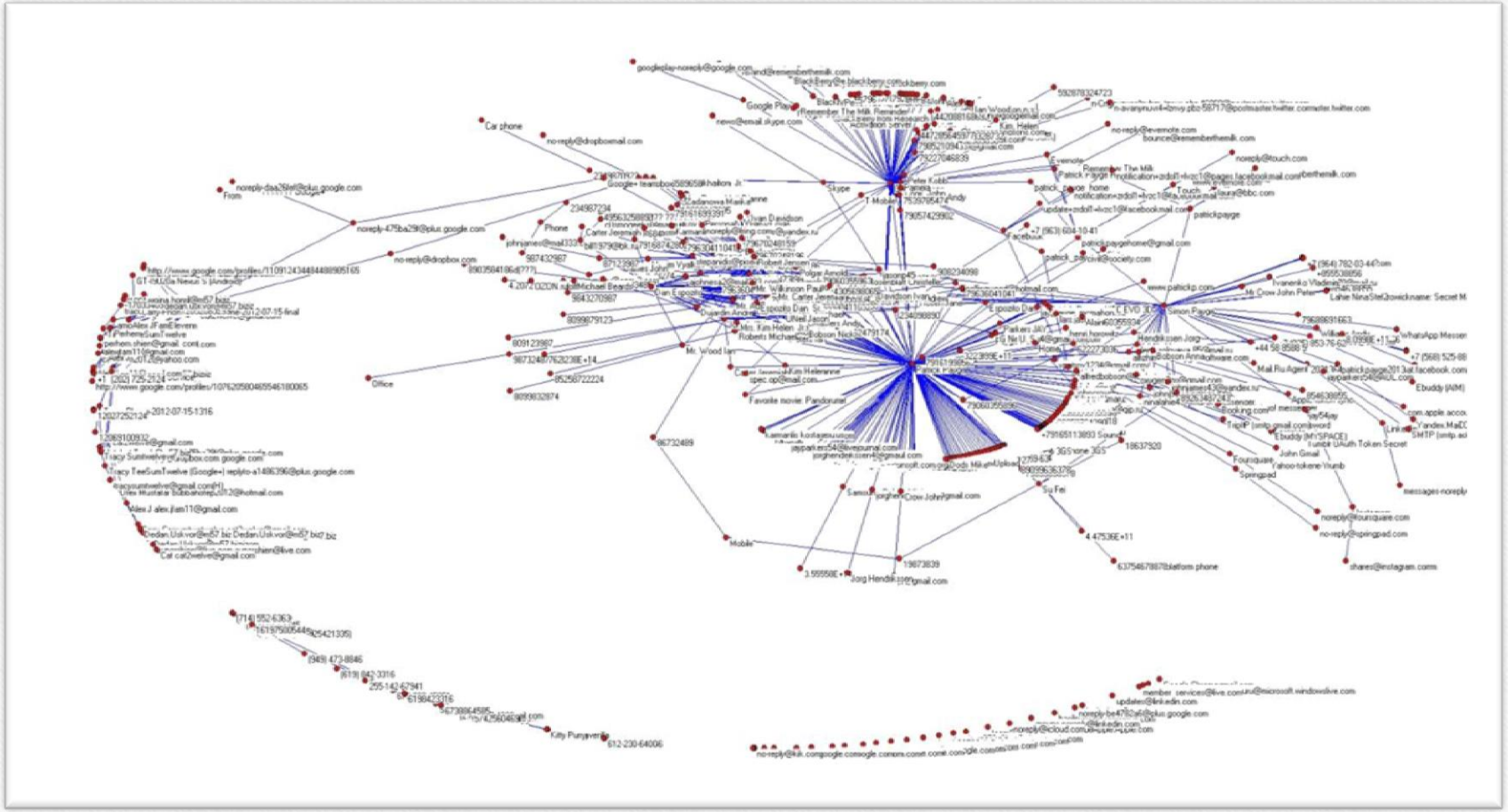
4.Mobile Phone Extracts

4.8 Digital Forensic Intelligence Analysis of Test Data

- The exported reports from the test data, the process of gaining intelligence from data can be undertaken.
- the test data Spreadsheet exports, all the CSV, XLS, and XLSX export reports were collated and manually merged to align columns and combined into one (very large) spreadsheet of all data from the extracts.
- A Fruchterman Reingold 2D entity link chart of was created, highlighting the interlinked nature of the 41 mobile device extracts

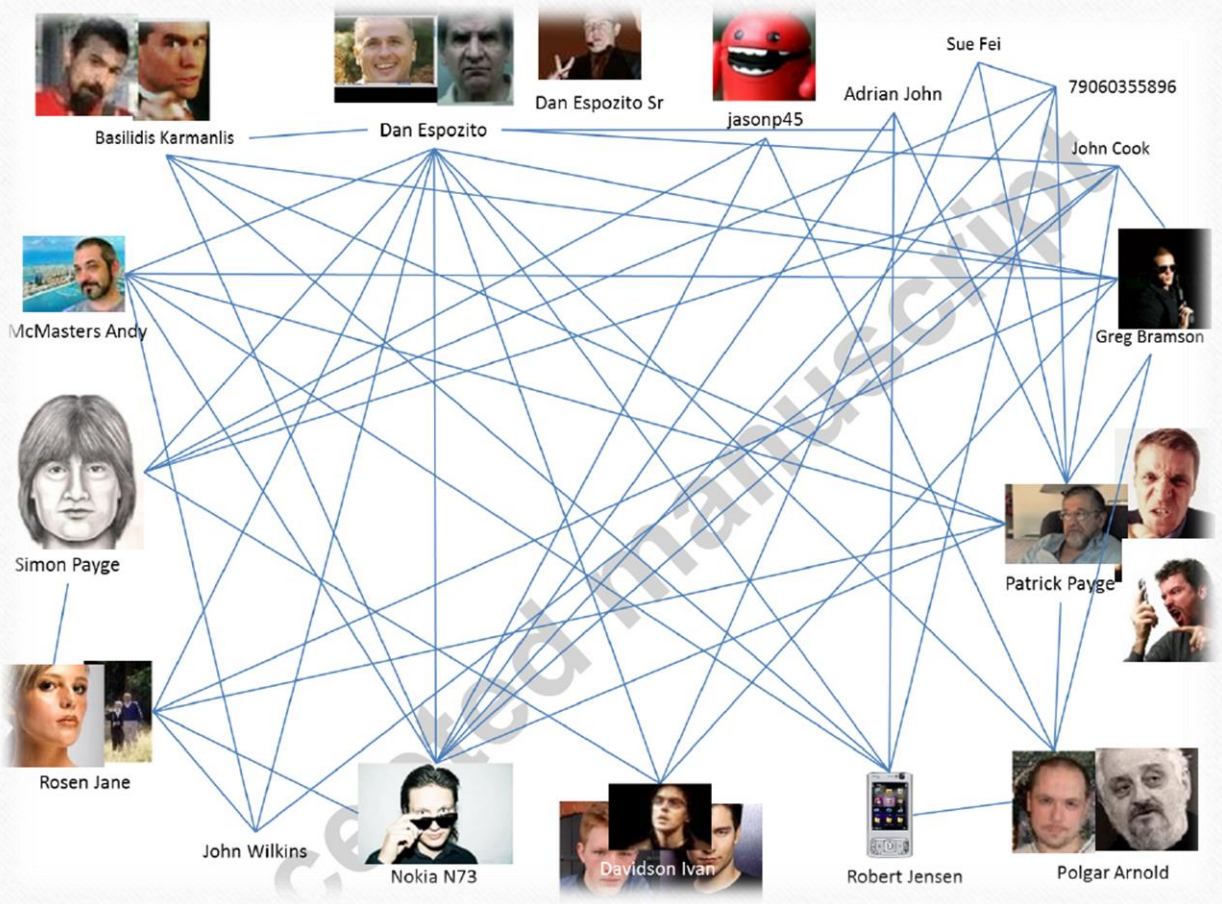
4.Mobile Phone Extracts

Entity Relationship chart of Oxygen Test Data using Pajek



4.Mobile Phone Extracts

Summarised Entity Link Chart of Oxygen Mobile Device Test Data Extracts



4.Mobile Phone Extracts

4.9 Summary of Test Data findings

- As a result of the test data experiments, it is concluded that there is potential benefits when exporting data to a common format.
- a process to reduce the volume and processing demands of mobile device extracts, by:

  - exporting the extracted data as spreadsheet (XLS/CSV/XLSX)

  - exporting pictures, videos, documents, and other files, and applying a digital forensic data reduction process

  - reducing the dimension of pictures, and thumbnailing video files.

Conclusion

- Conducting investigation involving the use of social networking services.
- it is integral that forensic practitioners begin by identifying the means that will be used to locate and acquire evidence (e.g. mobile devices).
- The volume of data on mobile devices is increasing, and is predicted to continue in future years.
- There is a potential that in 10 years' time, portable storage will be up to 512TB, and cloud storage data will also impact on the growing storage potential for users.

THANK YOU