A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis

Dr. Shahzad Saleem (SEECS-NUST Pakistan)
Professor Oliver Popov (DSV-SU Sweden)
Dr. Ibrahim Baggili (TCE-UNH USA)

KTH Applied Information Security Lab

Department of Computing, School of Electrical Engineering and Computer Sciences, NUST-Islamabad

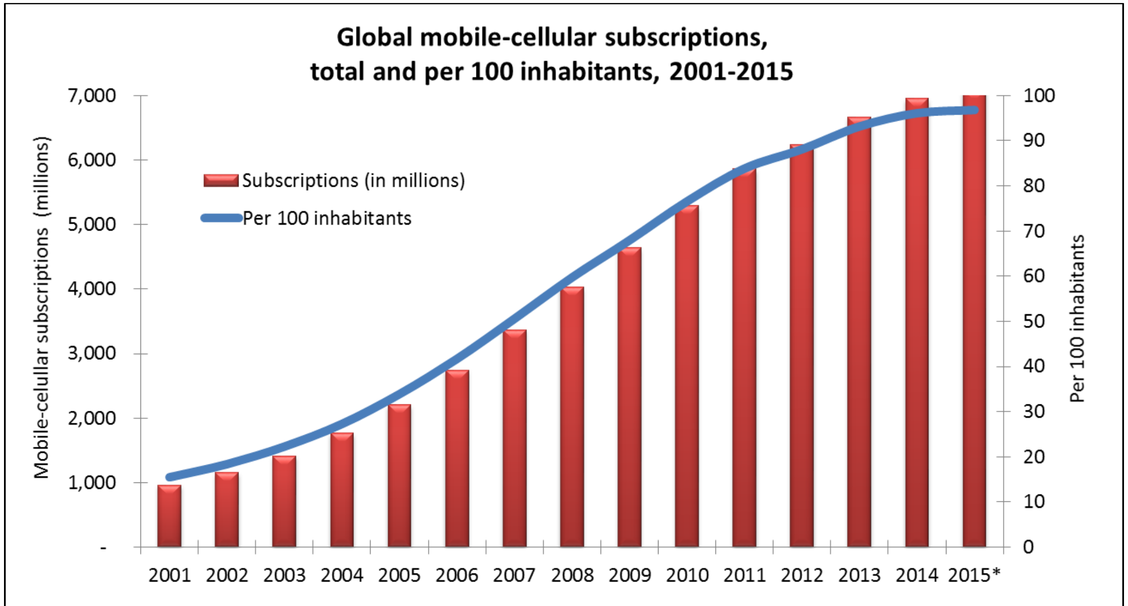
Agenda

- Introduction
- Related Work
- Theoretical Background
- Multi-Criteria Decision Analysis
- Conclusion

KTH
Applied
Information
Security
Lab

Introduction

- **Wide acceptance and deep penetration**
- **7 Billion subscriptions around the globe**



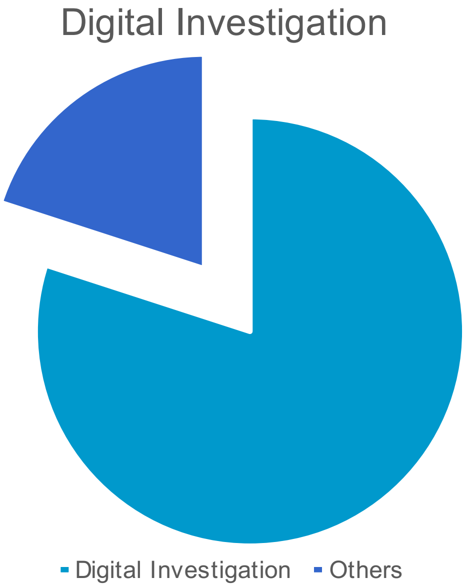
Note: * Estimate
Source: ITU World Telecommunication /ICT Indicators database

Introduction

- **Mobile Phones → Personal Digital Behavioural Archives.**

Introduction

- **80% of the cases have a digital side associated with them.**



KTH Applied Information Security Lab

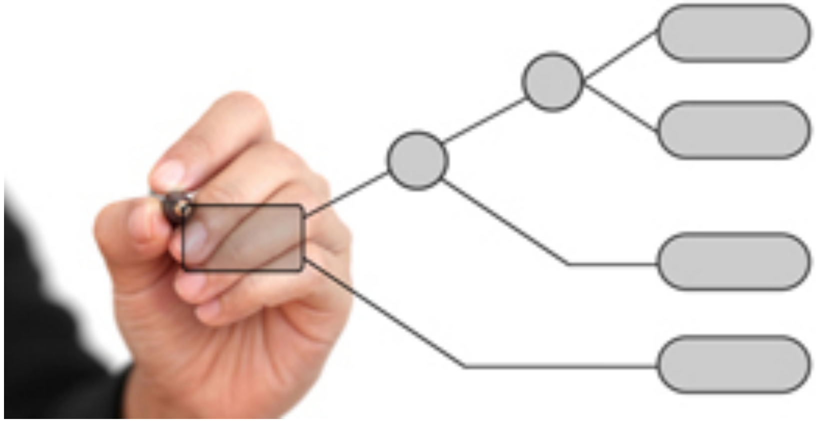
Introduction

- **Numerous mobile device forensics tools.**

KTH
Applied
Information
Security
Lab

Introduction

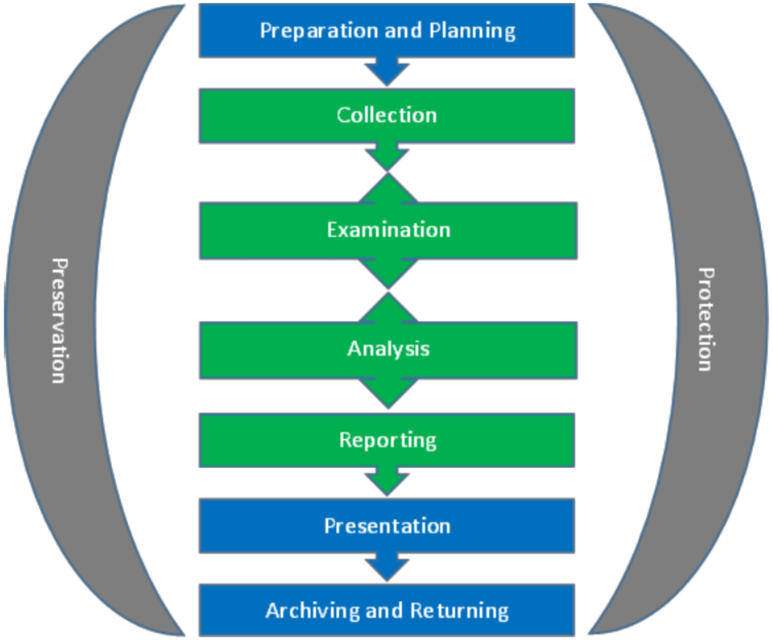
- A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis



KTH
Applied
Information
Security
Lab

Related Work

- **Preparation and planning phase of 2PasU.**
- **Vendor and TTP Evaluation (NIST)**



KTH
Applied
Information
Security
Lab

Related Work

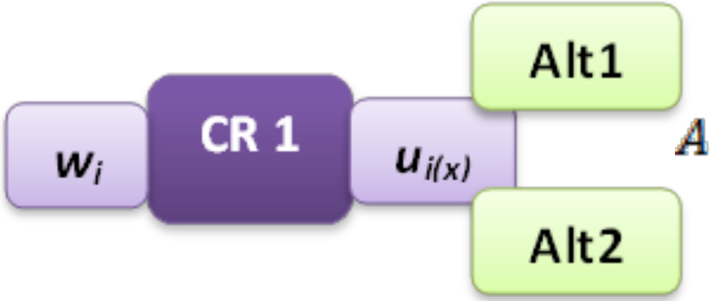
- Evaluation of some tools for extracting e-evidence from mobile devices
- Evaluating and Comparing Tools for Mobile Device Forensics using Quantitative Analysis
- Quantifying relevance of mobile digital evidence as they relate to case types: A survey and a guide for best practices

KTH
Applied
Information
Security
Lab

Theoretical Background

- Decision Analysis
  - Subjective probability
  - Appropriate measure of preference under uncertainty
- Probability
  - Ps = x/n
  - Used these proportions to connect different alternatives with each criteria in the MCD Model.

Theoretical Background



$$Alt1 > Alt2 + z_i / \sum_{i=1}^{n} |z_i|$$

- **We had 19 such nodes.**

$$U(x) = \sum_{i=1}^{n} w_i u_i(x)$$

MCD Analysis

- **MCD Analysis was based on performance and relevance.**
- **Performance**

ID	Criteria	Relational Connection (Equation 7)
1	Phonebook/Contacts	Alt1 = Alt2
2	Calendar Entries	Alt1 > Alt2 + 0.12472
3	Memo/Notes	Alt2 > Alt1 + 0.01156
4	Tasks/To-Do-Lists	Alt1 > Alt2 + 0.11483
5	SMS	Alt1 > Alt2 + 0.02105
6	EMS	Alt1 > Alt2 + 0.03867
7	MMS	Alt1 > Alt2 + 0.04998
8	Audio Calls	Alt1 > Alt2 + 0.09732
9	Video Calls	Alt1 = Alt2
10	Emails	Alt1 > Alt2 + 0.23780
11	URLs Visited	Alt1 = Alt2
12	Bookmarks/Favourites	Alt1 > Alt2 + 0.12480
13	Audio	Alt1 = Alt2
14	Video	Alt2 > Alt1 + 0.09048
15	Graphics/Pictures	Alt2 > Alt1 + 0.08895
16	Word	Alt1 = Alt2
17	Excel	Alt1 = Alt2
18	PowerPoint	Alt1 = Alt2
19	PDF	Alt1 = Alt2

ID	Criteria	Relational Connection (Equation 7)
1	Phonebook/Contacts	Alt1 > Alt2 + 0.00648
2	Calendar Entries	Alt1 > Alt2 + 0.07240
3	Memo/Notes	Alt1 > Alt2 + 0.05686
4	Tasks/To-Do-Lists	Alt1 > Alt2 + 0.06519
5	SMS	Alt1 = Alt2
6	EMS	Alt1 = Alt2
7	MMS	Alt1 > Alt2 + 0.08072
8	Audio Calls	Alt1 > Alt2 + 0.10663
9	Video Calls	Alt1 > Alt2 + 0.04106
10	Emails	Alt1 > Alt2 + 0.13805
11	URLs Visited	Alt1 = Alt2
12	Bookmarks/Favourites	Alt1 = Alt2
13	Audio	Alt1 > Alt2 + 0.14452
14	Video	Alt1 = Alt2
15	Graphics/Pictures	Alt1 = Alt2
16	Word	Alt1 > Alt2 + 0.08313
17	Excel	Alt1 > Alt2 + 0.04004
18	PowerPoint	Alt1 > Alt2 + 0.07919
19	PDF	Alt1 > Alt2 + 0.08573

KTH
Applied
Information
Security
Lab

MCD Analysis

- **Relevance**

Criteria (ID)	DT	RP	MD	CC	HMT	EE	CP
1	9.56	9.08	9.64	8.55	9.51	9.32	8.82
2	6.30	6.13	8.48	6.88	7.11	7.51	6.08
3	6.31	4.93	7.92	7.23	6.85	7.79	5.98
4	5.83	4.44	7.03	6.85	6.41	7.49	5.31
5	9.68	9.33	9.68	8.84	9.84	9.16	9.05
6	8.83	9.03	9.17	8.21	9.59	8.58	9.03
7	7.62	7.51	8.20	7.26	8.59	7.80	8.16
8	9.09	8.77	9.23	8.03	9.50	9.37	7.95
9	6.36	6.84	6.82	5.92	7.97	7.47	7.38
10	8.65	7.46	8.87	8.82	9.38	9.13	9.08
11	6.20	5.47	7.36	8.44	6.84	8.39	9.28
12	5.30	4.38	6.18	8.03	6.11	7.55	9.18
13	5.42	5.87	6.00	5.69	7.41	8.67	6.08
14	7.04	7.65	7.13	5.92	8.00	8.50	9.61
15	8.77	9.11	8.56	7.36	9.00	8.79	9.83
16	4.35	3.58	5.38	7.29	5.11	7.92	5.95
17	4.98	2.90	4.93	7.64	3.00	7.63	5.03
18	3.11	2.27	4.35	5.05	3.45	7.11	5.64
19	3.57	2.66	5.00	6.00	3.21	7.58	4.97

MCD Analysis

- **Relevance (Intra-Class Normalized)**

ID	DT	RP	MD	CC	HMT	EE	CP
1	0.34	0.37	0.29	0.29	0.32	0.29	**0.34**
2	0.23	0.25	0.26	0.23	0.24	0.23	**0.23**
3	0.23	0.20	0.24	0.25	0.23	0.24	**0.23**
4	0.21	0.18	0.21	0.23	0.21	0.23	**0.20**
5	0.37	0.36	0.36	0.36	0.35	0.36	**0.35**
6	0.34	0.35	0.34	0.34	0.34	0.34	**0.34**
7	0.29	0.29	0.30	0.30	0.31	0.31	**0.31**
8	0.59	0.56	0.57	0.58	0.54	0.56	**0.52**
9	0.41	0.44	0.43	0.42	0.46	0.44	**0.48**
10	1.00	1.00	1.00	1.00	1.00	1.00	**1.00**
11	0.54	0.56	0.54	0.51	0.53	0.53	**0.50**
12	0.46	0.44	0.46	0.49	0.47	0.47	**0.50**
13	0.26	0.26	0.28	0.30	0.30	0.33	**0.24**
14	0.33	0.34	0.33	0.31	0.33	0.33	**0.38**
15	0.41	0.40	0.39	0.39	0.37	0.34	**0.39**
16	0.27	0.31	0.27	0.28	0.35	0.26	**0.28**
17	0.31	0.25	0.25	0.29	0.20	0.25	**0.23**
18	0.19	0.20	0.22	0.19	0.23	0.24	**0.26**
19	**0.22**	**0.23**	**0.25**	**0.23**	**0.22**	**0.25**	**0.23**

$$w_d = \frac{w_i}{\sum_1^k w_i}$$

$$w_c = \frac{\sum_1^k w_i}{\sum_1^n w_j}$$

KTH
Applied
Information
Security
Lab

MCD Analysis

- **Relevance (Inter-Class Normalized)**

Class	DT	RP	MD	CC	HMT	EE	CP
PIM Entries	0.22	0.21	0.24	0.21	0.22	0.21	0.18
Messages	0.21	0.22	0.19	0.18	0.20	0.16	0.18
Call Logs	0.12	0.13	0.11	0.10	0.13	0.11	0.11
Emails	0.07	0.06	0.06	0.06	0.07	0.06	0.06
Internet History	0.09	0.08	0.10	0.12	0.09	0.10	0.13
Standalone Files	0.17	0.19	0.16	0.14	0.18	0.17	0.18
Application Files	0.13	0.10	0.14	0.19	0.11	0.19	0.15

$$w_d = \frac{w_i}{\sum_1^k w_i}$$

$$w_c = \frac{\sum_1^k w_i}{\sum_1^n w_j}$$

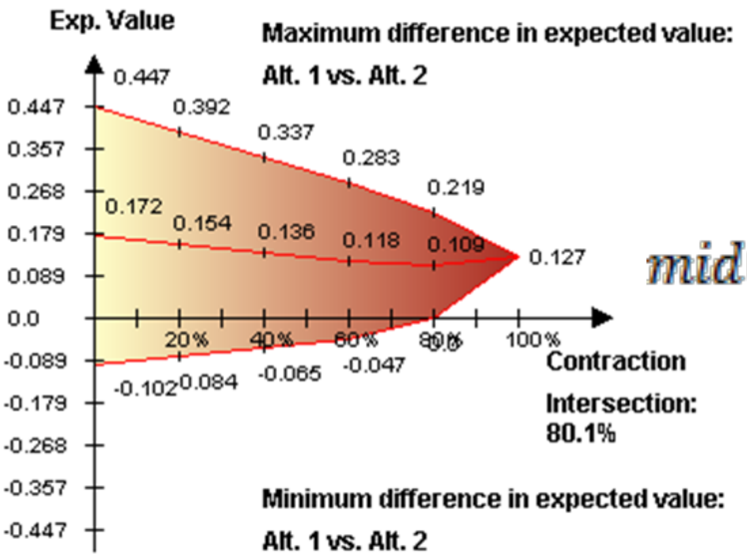
KTH
Applied
Information
Security
Lab

MCD Analysis

- **Evaluation**

$$\left[p-\frac{p}{20},p+\frac{p}{20}\right]$$

- **DecideIT converts a point estimate into a range.**
-

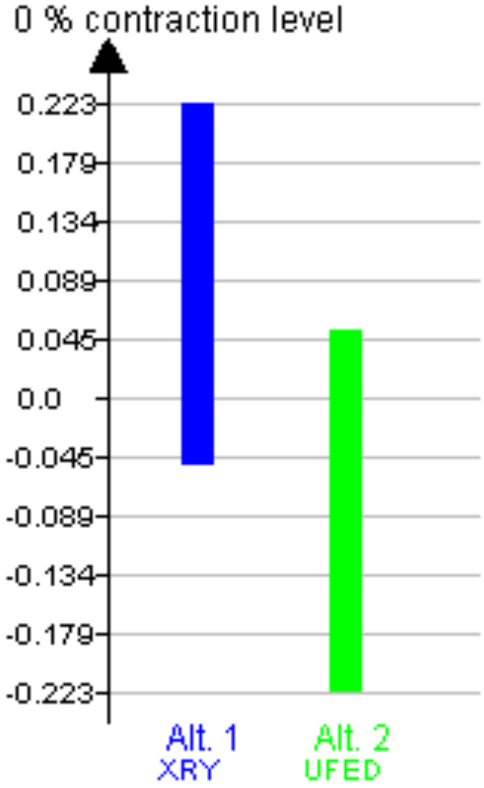


$$\delta_{12} = EU(A1) - EU(A2)$$

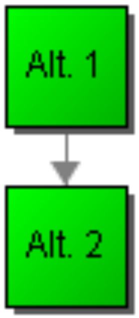
$$mid(\delta_{12}) = \frac{(max(\delta_{12}) + min(\delta_{12}))}{2}$$

MCD Analysis

- **Total and Cardinal Ranking**



Indifference interval: 10.0%

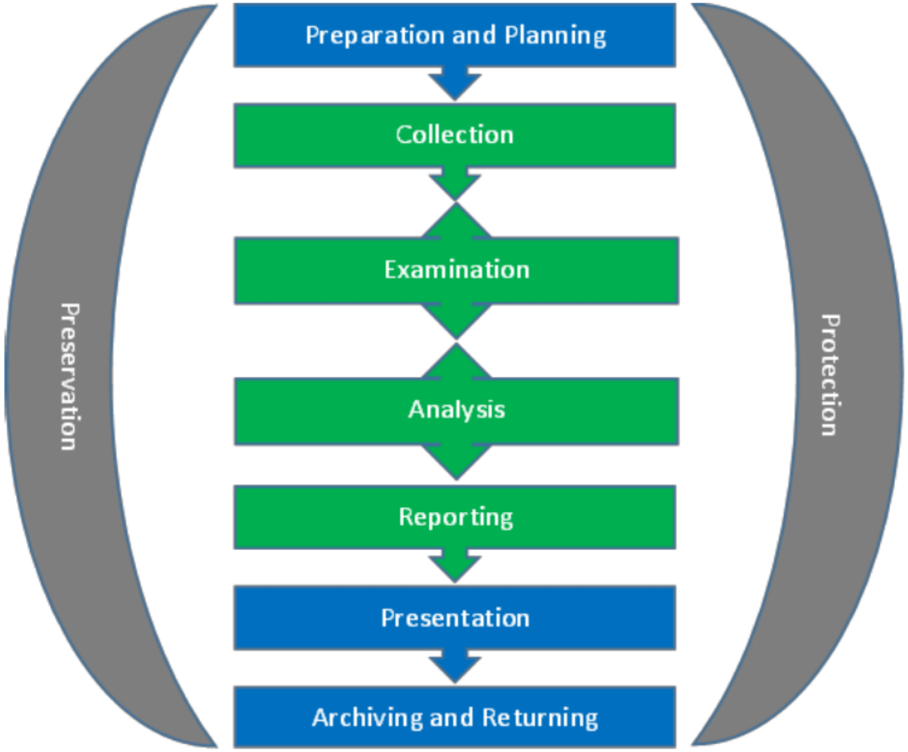


Conclusion

- We have a method which has been tested on a case study.
- We can extend it to include other emerging types of digital evidence and investigations involving digital forensics.
- One limitation of this method is that it requires continuous update to remain current while covering the maximum possible spectrum of digital forensics.

KTH
Applied
Information
Security
Lab

Conclusion (Current Work)



- **Collaboration and Suggestions are welcomed.**
  - **shahzad.saleem@seecs.edu.pk**
- **http://www.unhcfreg.com/#!datasetsandtools/c18k6**

KTH
Applied
Information
Security
Lab