University of BRISTOL

# Using AI for Supporting Cybercrime Investigations

Claudia Peersman

Awais Rashid

bristol.ac.uk

# Challenges for Law Enforcement

- Extent of the problem
  - 200 billion devices by 2020
- Identity in a digital world
  - fluid
  - dynamic
  - Adaptable
- Global aspect

University of BRISTOL
Bristol Cyber Security Group


# Potential of Artificial Intelligence for LE

- Automatically build, compare and detect user profiles on social media based on their linguistic fingerprint
- Detect false user profiles
- Detect suspicious conversations
- Automatic analysis of image and video content

University of BRISTOL
Bristol Cyber Security Group

# Applications of AI for Cybercrime Detection at UoB

- Online Child Protection
  - iCOP: identifying new CSAM on P2P networks
  - DAPHNE: detecting grooming in online social media

- Mass-marketing Fraud
  - DAPM: identifying deceptive messaging in advanced-fee and romance scams

- Financially motivated cyber crimes
  - AMoC: analyse the social and economic development of cyber criminal careers

Dashboard | Admin | Search

Logged in a

**Showing shared files for:**

| | |
|---|---|
| IP | 84.82.250.198 |

**Shared files**

Export for Excel | Export a

(1 of 5) 1 2 3 4 5 10

| | Name | SHA1 hash | Size | First seen | Last seen | Suspicious content | Suspicious filename | Known content | CSA | IP:port | GUID |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Amusing-Kids - Ksusha - 3 [pt | Y4BZSD4XTOFW7GHACG44K4DACEWS5HW5 | 60.9 MB | 2017-04-22 21:23:39 +0100 | 2017-04-22 21:23:39 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | ina2 - 5 [p | DKD4ECSWII7DNGSSS8LVZCLHOCKVBQLU | 82.3 MB | 2017-04-22 21:23:38 +0100 | 2017-04-22 21:23:38 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | rian Mouse | DL2LHK5H2TGT2GF6FKASM2PLAGD2YGFK | 41.3 MB | 2017-04-22 21:23:48 +0100 | 2017-04-22 21:23:48 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | 2 14yo Top | 2BFRHYU4RJILALGMCDOOR7HBNCSAYSRG | 25.5 MB | 2017-04-22 21:23:38 +0100 | 2017-04-22 21:23:38 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | tsc Pre 2Gi | 6GHOBXXBIMHFF6IQVPTGCB5P6SYZKSEO | 99.9 MB | 2017-04-22 21:23:37 +0100 | 2017-04-22 21:23:37 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | [ PTSC ] 11yo Racquel Show Ti | CWFNTZCOC4SJTC7BT2MMDRY5DWLN43LJ | 69.1 MB | 2017-04-22 21:23:37 +0100 | 2017-04-22 21:23:37 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | 11Yo & 14Yo Russian Preteens | REVOQPSVSQ3WYNJXFUYR4AXAVFBIQ4ZQ | 76.1 MB | 2017-04-22 21:23:37 +0100 | 2017-04-22 21:23:37 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | Xxx Porn Pussy Teen 10Yo Sex | Z4YBDHKUFVNGOYOCHXNDKKKQVZ3MSZIW | 194.9 kB | 2017-04-23 01:14:47 +0100 | 2017-04-23 01:14:47 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | !!! - 1st-Studio Siberian Mouse | UY3EKL72CJSMA3N552MDNZP622M5TFRY | 103.2 kB | 2017-04-22 21:23:47 +0100 | 2017-04-22 21:23:47 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |
| | !!NEW!! tv1c Georgia Peach T | PM6CNRAHFECEKDKIL3QSMQSVOQYTSXMB | 26.7 MB | 2017-04-22 21:23:36 +0100 | 2017-04-22 21:23:36 +0100 | | X | | | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED |

(1 of 5) 1 2 3 4 5 10

**Connection details**

| | |
|---|---|
| IP | 84.82.250.198 |
| Location | Amersfoort / NL |

**Related connections**

**Connections related to IP 84.82.250.198**

1

| IP:port | GUID | |
|---|---|---|
| 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED1AA3 | View |

1

**Comments**

University of BRISTOL
Bristol Cyber Security Group

Export all for Excel | Export all as CSV | Export page for Excel

(1 of 124) 1 2 3 4 5 6 7 8 9 10 5

| # known files | # files | IP:port | GUID | Last seen | Location |
|---|---|---|---|---|---|
| 0 | 9 | 173.49.48.41:6346 | 877FBCEA8524504990C9241CCACEE0A4 | 2017-04-22 21:18:54 +0100 | Broomall / Pennsylvania / US |
| 0 | 1 | 77.205.191.167:6346 | 7DE2BC0F19C7BF4DA84DB8CD68309FC0 | 2017-04-26 11:07:33 +0100 | / / FR |
| 0 | 1 | 74.193.96.65:58987 | 261C8AA7582BA24DB3AFBCD6E6CCD4E6 | 2017-04-22 21:21:38 +0100 | Gainesville / Texas / US |
| 0 | 1 | 78.130.76.183:6346 | 6130FD633B49A24FBD7A7115E2FF024E | 2017-04-23 20:26:35 +0100 | / / PT |
| 0 | 13 | 88.183.159.229:6346 | 6215F0D85C429945B56329B416203038 | 2017-04-26 12:47:43 +0100 | Marles-les-mines / Nord-Pas-de-Calais |

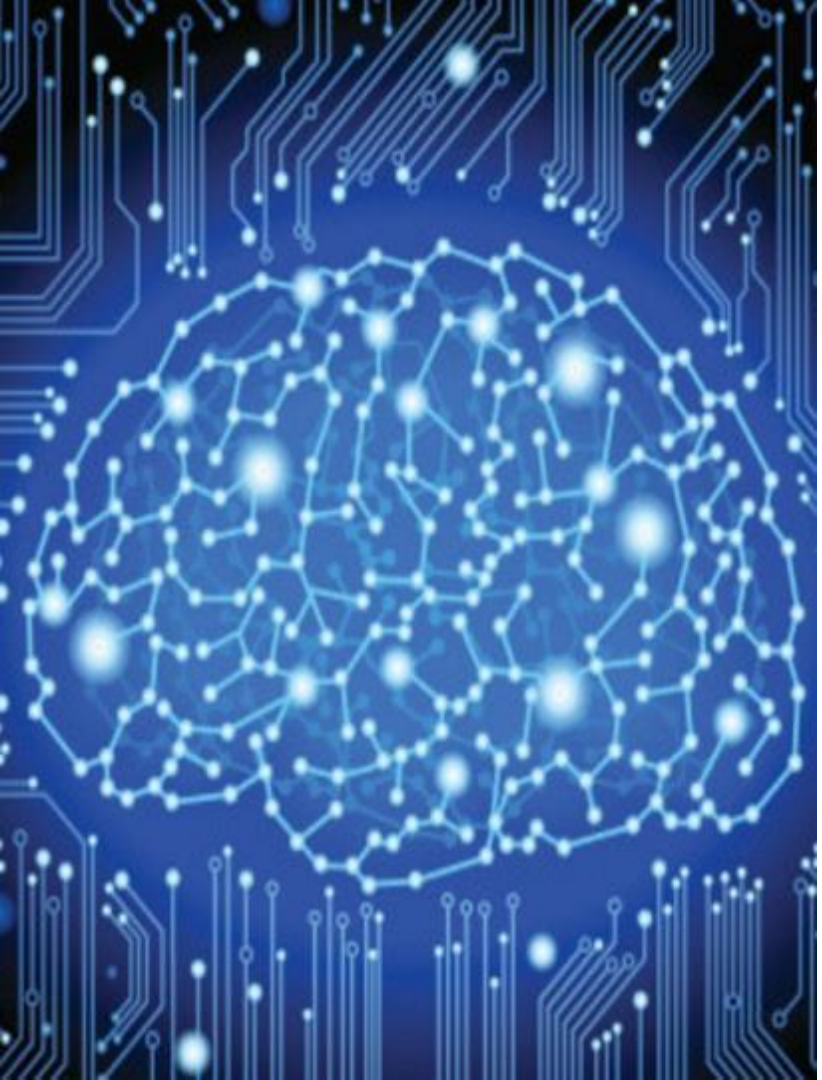
(1 of 124) 1 2 3 4 5 6 7 8 9 10 5

| # known files | # files | IP:port | GUID | Last seen | Location | | Hidden on |
|---|---|---|---|---|---|---|---|
| 0 | 47 | 84.82.250.198:6346 | D6505EF955D0F446939740E9BBED1AA3 | 2017-04-26 12:28:44 +0100 | Amersfoort / Utrecht / NL | View | 2017-04-26 11:50: |


iCOP’s false positive rates:

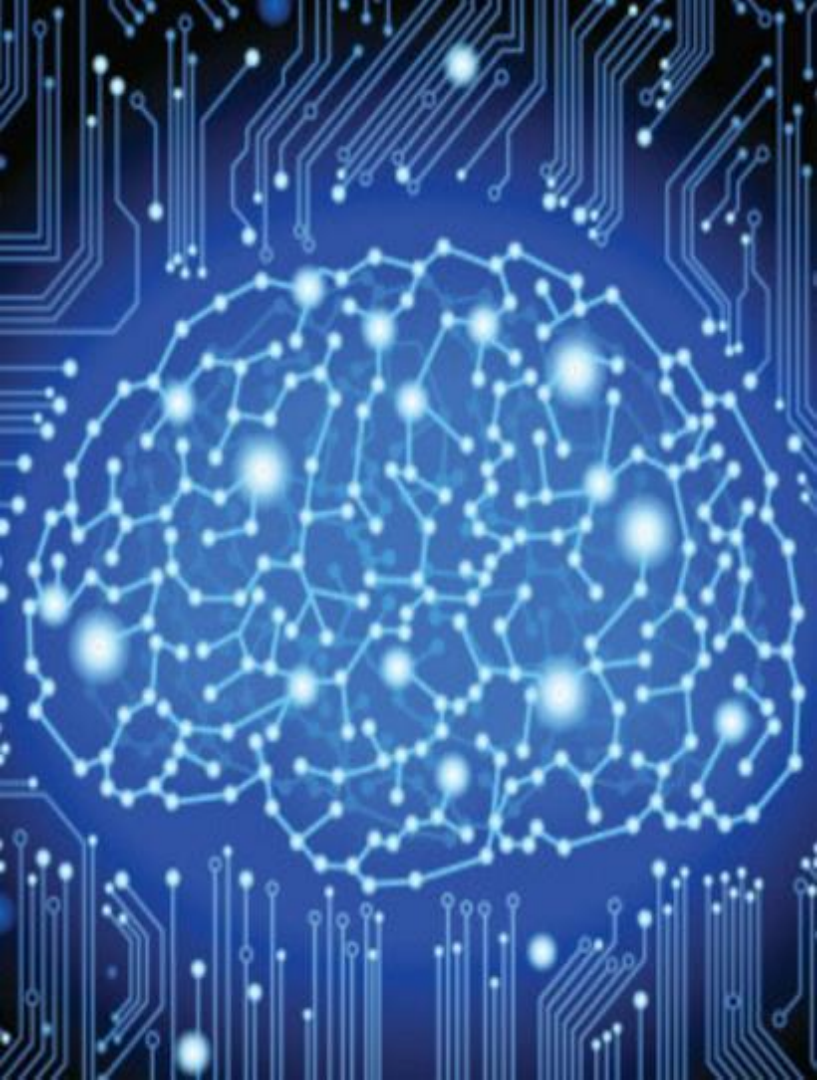
- Images 7.9%
- Videos 4.3%

University of BRISTOL
Bristol Cyber Security Group



# Benefits of Artificial Intelligence

- Match/outperform human performance
  - fraction of time
  - no human limitations
  - consistent performance
- Automatically detect victims at acute risk
- Assign degrees of importance and urgency to items of evidence in order to assess cyber offenders' potential danger to society
- Find useful evidence in a timely manner
- BUT: final decisions are made by human experts



# Challenges of Artificial Intelligence

- Projects like iCOP require a multi-stakeholder approach:
  - European Safer Internet Programme
  - Interpol & other LE
  - Multi-disciplinary academic expertise
- Training data is essential: both quality and quantity
- Forecasting is critical to get a step ahead of cybercriminals instead of being a step behind

# Research Papers

***iCOP: live forensics to reveal previously unknown criminal media on P2P networks***
Peersman, C., Schulze, C., Rashid, A., Brennan, M. & Fischer, C. 09/2016 In : Digital Investigation. 18, p. 50-64, 15 p.

***Ethical and Social Challenges with developing Automated Methods to Detect and Warn potential victims of Mass-marketing Fraud (MMF)***
Whitty, M, Edwards, M, Levi, M, Peersman, C, Rashid, A, Sasse, MA, Sorell, T & Stringhini, G, 2017. in:*Proceedings of the 26th International Conference on World Wide Web Companion, Perth, Australia, April 3-7, 2017*., pp. 1311-1314

***Scamming the Scammers: Towards Automatic Detection of Persuasion in Advance Fee Frauds***
Edwards, MJ, Peersman, C & Rashid, A, 2017. In: *Proceedings of the 26th International Conference on World Wide Web Companion, Perth, Australia, April 3-7, 2017*., pp. 1291-1299

***A systematic survey of online data mining technology intended for law enforcement***
Edwards, M., Rashid, A., Rayson, P. 09/2015 In: ACM Computing Surveys. 48 (1), 15 p.

***Conversation Level Constraints on Pedophile Detection in Chat Rooms***
Peersman, C, Vaassen, F, Van Asch, V & Daelemans, W, 2012. In: *CLEF: Online Working Notes/Labs/Workshop*.