



LEEDS
BECKETT
UNIVERSITY

Citation:

Lambourne, AD and Elliott, JR and Miller, S and Collins, L and Schreuders, ZC (2018) Software Pilot and User Guide EWT: Chat Log Grooming Detection. Manual. CSI Centre Leeds Beckett University. (Unpublished)

Link to Leeds Beckett Repository record:

<https://eprints.leedsbeckett.ac.uk/id/eprint/5078/>

Document Version:

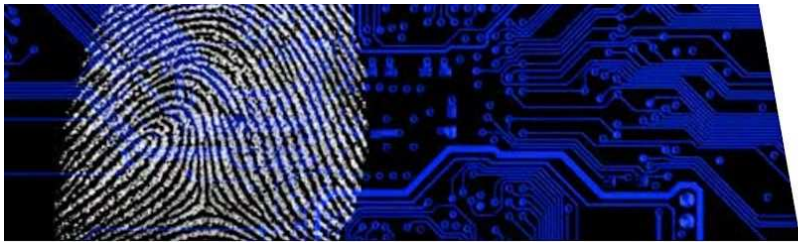
Monograph (Published Version)

The aim of the Leeds Beckett Repository is to provide open access to our research, as required by funder policies and permitted by publishers and copyright law.

The Leeds Beckett repository holds a wide range of publications, each of which has been checked for copyright and the relevant embargo period has been applied by the Research Services team.

We operate on a standard take-down policy. If you are the author or publisher of an output and you would like it removed from the repository, please [contact us](#) and we will investigate on a case-by-case basis.

Each thesis in the repository has been cleared where necessary by the author for third party copyright. If you would like a thesis to be removed from the repository or believe there is an issue with copyright, please contact us on openaccess@leedsbeckett.ac.uk and we will investigate on a case-by-case basis.



Software Pilot and User Guide EWT: Chat Log Grooming Detection

Andrew Lambourne, John Elliott, Stephen Miller, Lewis Collins, and Z. Cliffe Schreuders

Leeds Beckett University and West Yorkshire Police

2018

This software is currently available for police use. See below for details on obtaining EWT and participating in the pilot.

The CARI Project

The CARI Project is a large-scale collaboration between West Yorkshire Police and the Cybercrime and Security Innovation Centre (CSI Centre) at Leeds Beckett University. The CARI Project aims to improve and incorporate an evidence-based approach into the policing of digital forensics and cybercrime investigations. An extensive needs assessment of UK policing and cybercrime and digital evidence was conducted to understand the current situation, and to identify needs across the force. The CARI Project also involved implementing a training and research programme that has impacted the capability of the digital forensics and cyber units within West Yorkshire Police to engage in research. This needs assessment and research training led to the development of a set of research proposals, which were scored and selected. Subsequently, academics and police staff co-produced 9 research and development workstreams: a framework for seizure, preservation and preservation of cloud evidence; automated forensic analysis; image linkage for victim identification and framework for image fingerprint management; automated grooming detection; frontline officer awareness development and decision support mobile app; assessment of methods of cyber training; an evaluation of the role of the Digital Media Investigator within WYP; and characteristics of victims of cybercrime. Each of these projects were designed to address needs within law enforcement and outputs include evidence-based procedures, new capabilities such as software/algorithms, and actionable intelligence.

This work was supported by a Police Knowledge Fund grant, administered by the Home Office, College of Policing, and the Higher Education Funding Council for England (HEFCE).



LEEDS
BECKETT
UNIVERSITY



WEST YORKSHIRE
POLICE

EWT: Chat Log Grooming Detection

The aim of this work is the creation of tools and techniques to detect and flag evidence of predatory behaviour by scanning chat and other social media logs extracted from seized equipment. Although the research literature proposes techniques for modelling and detecting “luring” dialogues (Olson et al., 2007; Leatherman, 2009), Digital Forensics Units (DFU) typically rely on manual review, searching, and simple keyword lists. Based on analysis of this information and the associated academic papers, a series of predatory speech acts were identified as being relevant to the automated detection of grooming. The EWT scanning algorithm was tuned and refined first against PJ logs and also against real world data.

The result is a software tool that can be used by investigators to automate log-file screening to quickly filter through chat logs to identify evidence. The approach is sufficiently generic to allow the same tool to be used with different lexicons to detect other dialogues of concern such as cyber-stalking and radicalisation or terrorist recruitment.

Current status: we are piloting the software in a number of forces (started May 2018). UK forces are invited to contact DCI Vanessa Smith (vanessa.smith@westyorkshire.pnn.police.uk) and Dr Z. Cliffe Schreuders (c.schreuders@leedsbeckett.ac.uk) to join the pilot.

Contents

[How to install](#)

[Starting EWT](#)

[How the software is used](#)

[Step 1\) Import chat logs.](#)

[Step 2\) Process chat logs.](#)

[Step 3: View results.](#)

[Step 4\) Providing feedback.](#)

[Information sheet](#)

[Consent statement](#)

How to install

EWT has been developed and tested on Linux and Windows.

Step 1) Install Anaconda, Python 2.7 version

Anaconda can be downloaded from here:

<https://www.anaconda.com/download>

This includes all the various libraries you need to run EWT.

Alternatively, you could manually install Python 2.7, Qt5, and all the required Python modules, including `xlswriter`, `argparse`, and `hashlib`. However, installing Anaconda is the recommended approach.

Step 2) Save the EWT software to a location of your choosing (such as a folder in your home directory). If you received EWT as a zip file, this involves extracting the contents of that file to a PC.

Note: you will launch the software from this folder. If you want to add a shortcut to your desktop, you can copy the `ewt_windows` shortcut to your desktop, then edit the shortcut by right clicking the copy of the shortcut, selecting `Properties`, and the `Target` field can be edited to insert the full path where you have saved EWT just before `"ewt_gui.py"`. For example: it becomes ...`"start pythonw C:\EWT\ewt_gui.py"`...

Starting EWT

On Windows with Anaconda, simply double click on `"ewt_windows"`



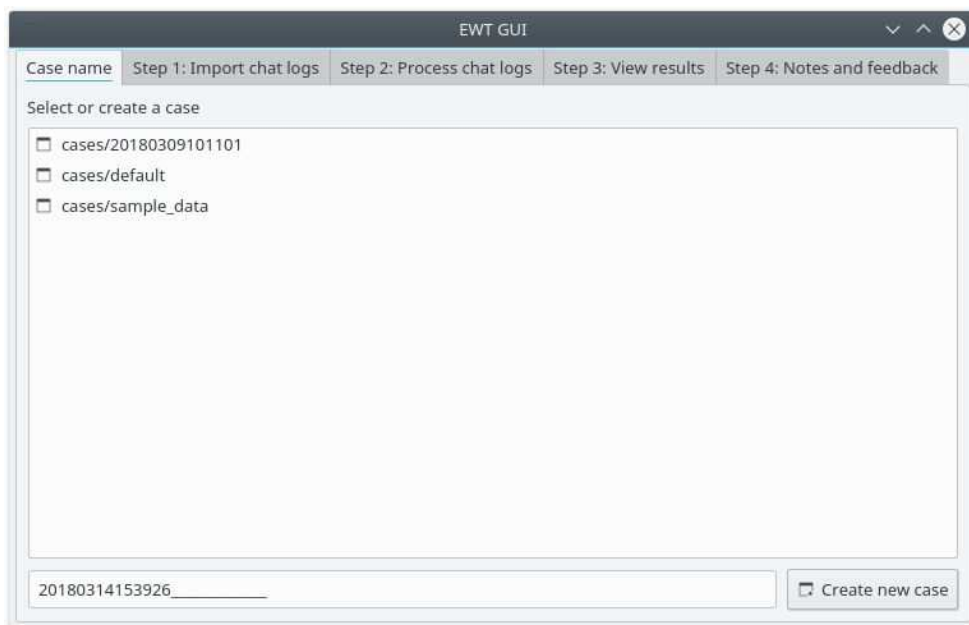
On Linux with Anaconda, simply run `"ewt_linux.sh"`

Or on Windows or Linux with manual install, start a bash shell in the EWT directory and run:

```
python ewt_gui.py
```

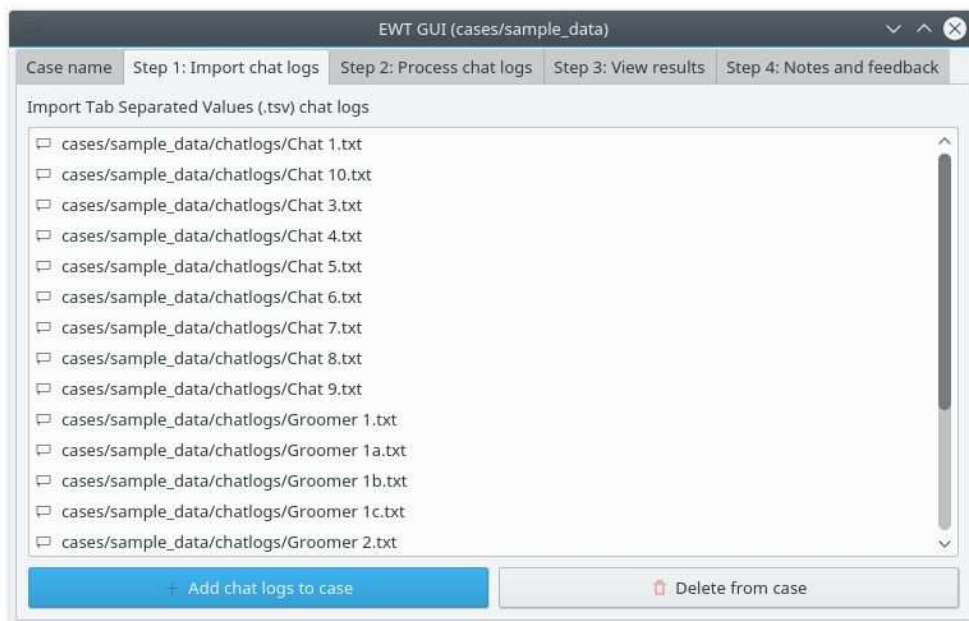
How the software is used

First, create a case.



Step 1) Import chat logs.

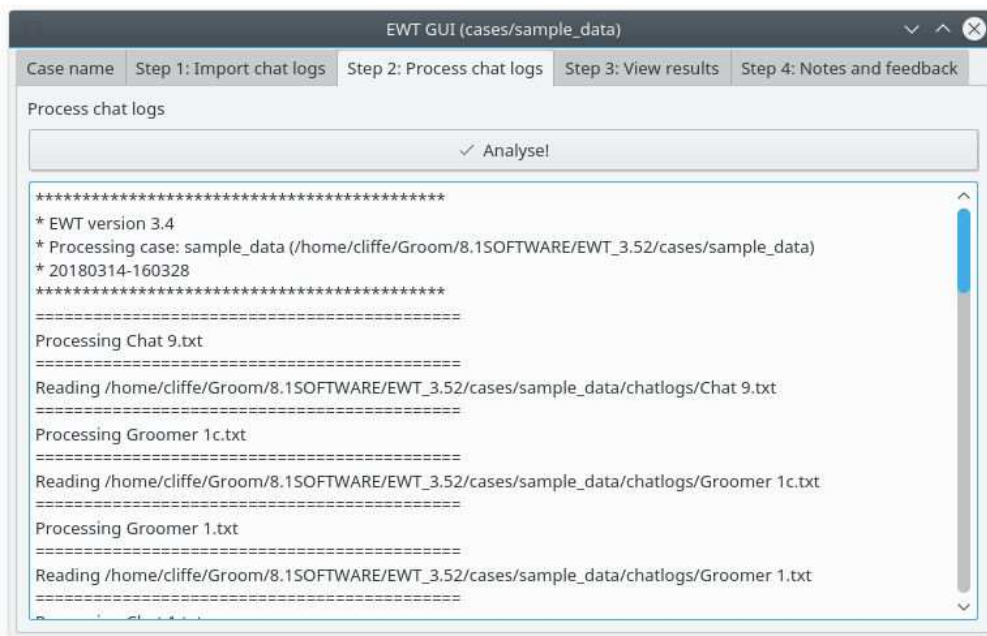
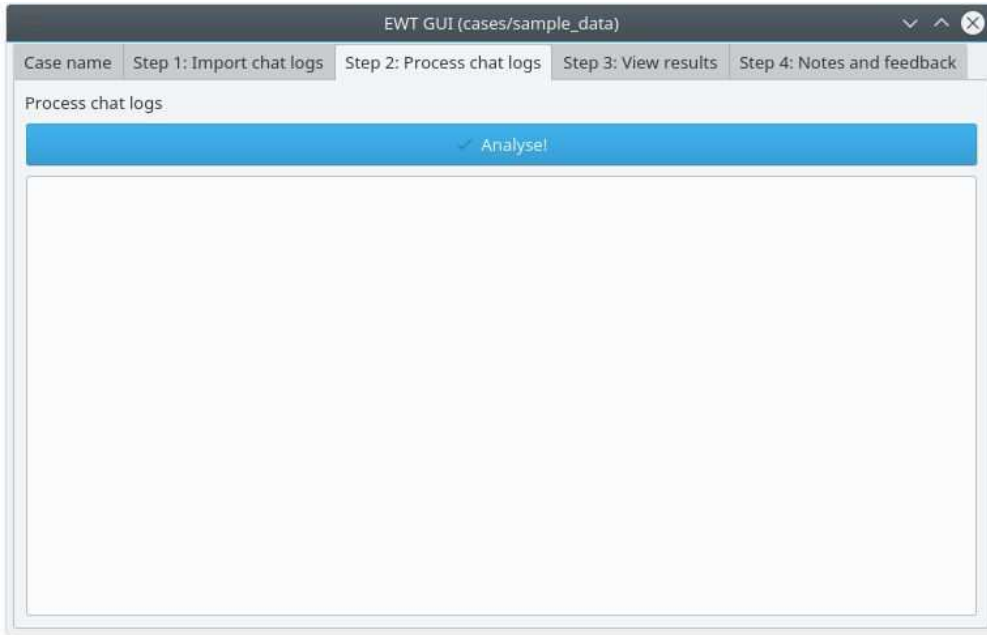
The tool imports TSV exports, which most forensic tools can easily export chat logs to.



Step 2) Process chat logs.

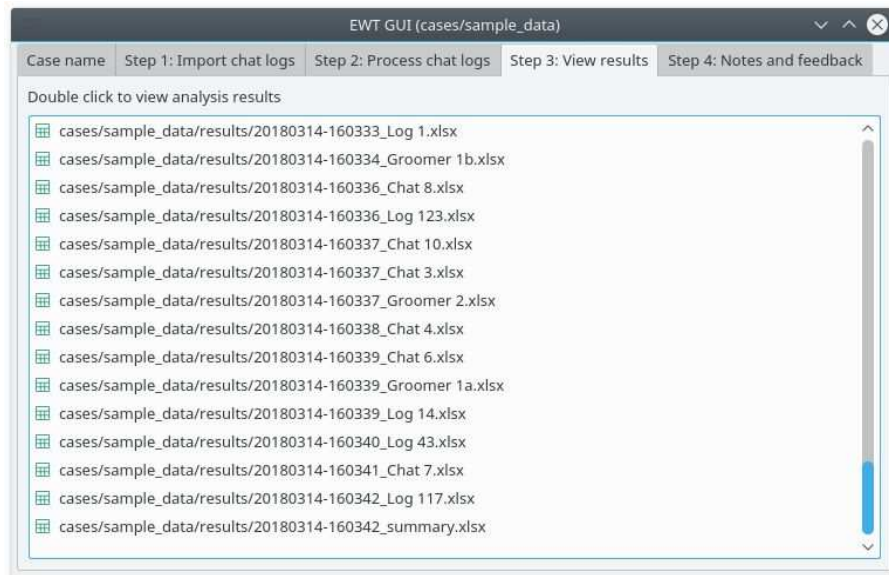
Simply click "Analyse!"

Every message is analysed and results are saved.



Step 3: View results.

Simply double click to open each results file, which are spreadsheets with filters for quickly viewing and making sense of the chat logs.



Every message has been analysed and assigned a matching *speech act* category. Categories include:

- **Direct Sexual:** explicitly sexual
- **Indirect Sexual:** sexual innuendo and desensitisation
- **Age:** related to age
- **Pleading/Demanding:** begging, pleading, and demanding
- **Approach:** in person meet ups and initiating contact
- **Groomers:** groomers talking to groomers
- **Personal:** exchanging personal information, including discussing appearance, family, home, and discussing photos, webcams
- **Compliments:** appearance compliments
- **Negative:** refusals, and negative responses to advances
- **Trust:** related to building trust, and reassuring
- **Isolation:** isolation from others

A summary document (“...summary.xlsx”) provides an overview of the results of analysis. This view can help to provide insights such as one sided conversations, and chat files with a high number of hits against these categories.

1	Filename	Participants	Direct_Sexual	Indirect_Sexual	Age	Pleading_Demandin	Approach	Personal	Compliments	Insults	True	Isolation	Categorized	Message Total
41														
42	Log117.txt	<Victim>	4	0	0	0	0	0	0	0	2	0	0	6
43	Log117.txt	<Groomer>	38	0	0	0	0	9	2	0	0	0	57	358
44														
45	Chat 9.txt	<Victim>	77	16	6	4	3	33	8	28	23	2	200	1119
46	Chat 9.txt	<Groomer>	36	9	3	1	5	7	2	13	16	3	89	1287
47														
48	Log1.txt	<Victim>	1	1	1	0	0	0	0	7	0	0	10	110
49	Log1.txt	<Groomer>	35	13	0	1	1	0	2	1	0	1	54	161
50														
51	Log43.txt	<Victim>	0	0	4	0	0	0	0	0	0	0	4	105
52	Log43.txt	<Groomer>	32	3	0	1	0	2	1	3	0	1	43	141
53														
54	Groomer1.txt	<Suspect>	24	3	3	2	0	7	5	3	11	0	58	244
55	Groomer1.txt	<Victim>	30	5	4	2	2	3	0	0	11	2	59	236
56														
57	Log14.txt	<Victim>	0	0	0	0	0	0	0	0	0	0	0	73
58	Log14.txt	<Groomer>	18	5	0	0	0	0	1	3	0	0	27	104
59														
60	Chat1.txt	<Suspect>	18	5	0	1	0	0	4	0	3	0	31	147
61	Chat1.txt	<Victim>	7	3	7	2	0	0	0	3	2	0	30	177

Drilling down, each chat log is stored in a separate spreadsheet, coded against the speech acts:

1	Line No	Participant	TimeStamp	Message	Category	Category Colour
2	0		<08/22/06 12:15:36 AM>		Approach	Red
3	1		<08/22/06 12:15:36 AM>		Approach	Red
4	2		<08/22/06 12:15:36 AM>		Age	Red
5	3		<08/22/06 12:15:53 AM>			Black
6	4		<08/22/06 12:15:53 AM>			Black
7	5		<08/22/06 12:16:12 AM>			Black
8	6		<08/22/06 12:16:18 AM>			Black
9	7		<08/22/06 12:16:37 AM>			Black
10	8		<08/22/06 12:17:08 AM>		Indirect_Sexual	Red
11	9		<08/22/06 12:17:22 AM>		Personal	Amber
12	10		<08/22/06 12:17:22 AM>		Approach	Red
13	11		<08/22/06 12:18:19 AM>			Black
14	12		<08/22/06 12:18:33 AM>			Black
15	13		<08/22/06 12:18:15 AM>		Personal	Amber
16	14		<08/22/06 12:20:17 AM>			Black
17	15		<08/22/06 12:21:11 AM>		Direct_Sexual	Red
18	16		<08/22/06 12:21:19 AM>		Personal	Amber
19	17		<08/22/06 12:21:40 AM>			Black
20	18		<08/22/06 12:22:13 AM>		Direct_Sexual	Red
21	19		<08/22/06 12:22:55 AM>		Direct_Sexual	Red
22	20		<08/22/06 12:23:47 AM>			Black
23	21		<08/22/06 12:24:12 AM>		Personal	Amber
24	22		<08/22/06 12:26:18 AM>		Direct_Sexual	Red
25	23		<08/22/06 12:26:42 AM>			Black
26	24		<08/22/06 12:27:28 AM>			Black
27	25		<08/22/06 12:29:16 AM>			Black
28	26		<08/22/06 12:29:50 AM>		Indirect_Sexual	Red
29	27		<08/22/06 12:31:20 AM>		Compliments	Amber
30	28		<08/22/06 12:31:41 AM>		Direct_Sexual	Red
31	29		<08/22/06 12:33:03 AM>		Direct_Sexual	Red
32	30		<08/22/06 12:33:25 AM>			Black

(Contents in these images have been censored.)

We classify the first six categories (Direct Sexual, Indirect Sexual, Age, Pleading/Demanding, Approach, and Groomers) as “Red” (highest concern), the others as “Amber”.

For a quick view of the highest concern messages, messages can be filtered to “Red” traffic light:

The image shows a spreadsheet filter menu for the 'Category' column. The menu is open, displaying a list of categories: Approach, Approach, Age, Indirect_Sexual, Approach, Direct_Sexual, Direct_Sexual, Direct_Sexual, Direct_Sexual, Indirect_Sexual, Direct_Sexual, Direct_Sexual, Direct_Sexual, Direct_Sexual, Direct_Sexual, Indirect_Sexual, Indirect_Sexual, Indirect_Sexual, Direct_Sexual, Direct_Sexual, Direct_Sexual, Indirect_Sexual, Direct_Sexual, Direct_Sexual, Indirect_Sexual, Direct_Sexual, Direct_Sexual, Indirect_Sexual. The 'Red' category is selected, indicated by a blue square next to it. The 'Amber' and 'Black' categories are unselected. The 'All' button is also visible at the bottom of the menu.

Likewise, messages can be filtered down at the category level, to detect attempts to meet:

The screenshot shows a table of messages with a filter dialog box overlaid. The dialog box has the following options:

- Sort Ascending
- Sort Descending
- Top 10
- Empty
- Not Empty
- Standard Filter...
- Search items...
- (empty)
- Age
- Approach
- Compliments
- Direct_Sexual
- All

The 'Approach' category is selected in the dialog box.

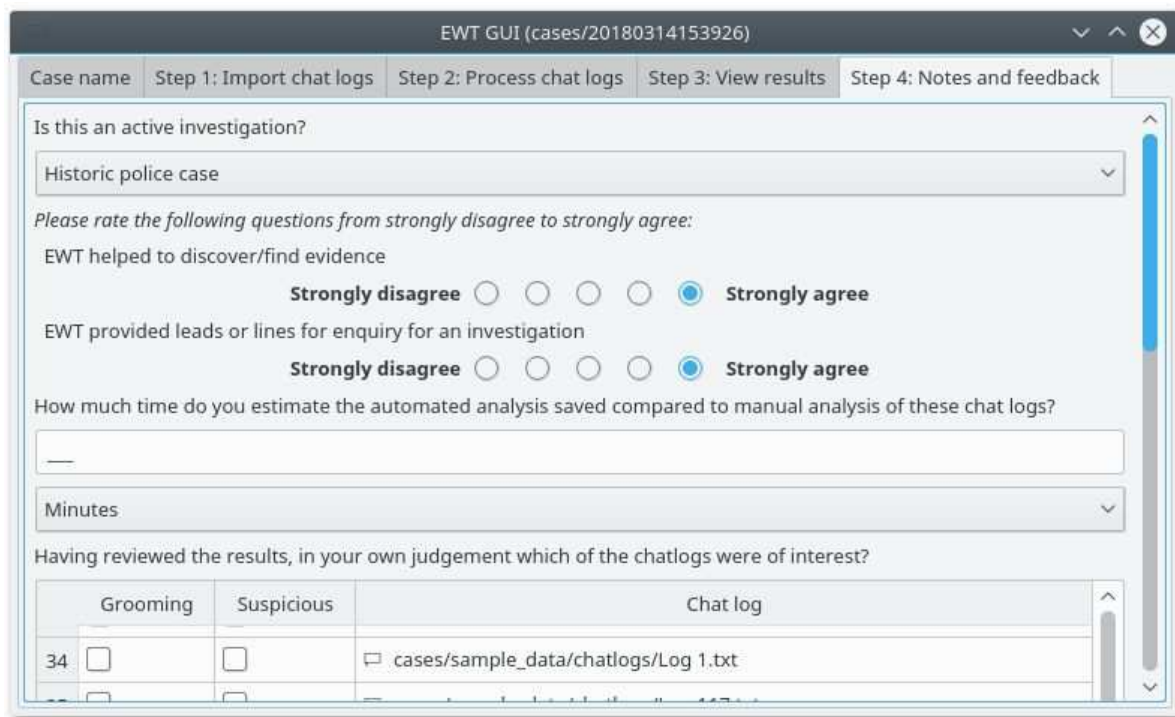
Or focusing on sexual comments:

Line No	Participant	TimeStamp	Message	Category	Category Colour
8		<08/22/06 12:17:08 AM>		Indirect_Sexual	Red
15		<08/22/06 12:21:11 AM>		Direct_Sexual	Red
18		<08/22/06 12:22:13 AM>		Direct_Sexual	Red
19		<08/22/06 12:22:55 AM>		Direct_Sexual	Red
22		<08/22/06 12:26:18 AM>		Direct_Sexual	Red
26		<08/22/06 12:29:50 AM>		Indirect_Sexual	Red
28		<08/22/06 12:31:41 AM>		Direct_Sexual	Red
29		<08/22/06 12:33:03 AM>		Direct_Sexual	Red
37		<08/22/06 12:34:47 AM>		Direct_Sexual	Red
41		<08/22/06 12:38:00 AM>		Direct_Sexual	Red
48		<08/22/06 12:40:31 AM>		Direct_Sexual	Red
49		<08/22/06 12:40:45 AM>		Indirect_Sexual	Red
50		<08/22/06 12:41:18 AM>		Indirect_Sexual	Red
51		<08/22/06 12:41:28 AM>		Indirect_Sexual	Red
61		<08/22/06 12:45:52 AM>		Indirect_Sexual	Red
63		<08/22/06 12:46:19 AM>		Direct_Sexual	Red
66		<08/22/06 12:47:48 AM>		Direct_Sexual	Red
76		<08/22/06 12:53:54 AM>		Direct_Sexual	Red
77		<08/22/06 12:54:02 AM>		Direct_Sexual	Red

Step 4) Providing feedback.

We ask that during the pilot, police users provide us with feedback regarding their use of EWT.

Please complete a short survey within the software, **for each and every case during the pilot period**. There are only a few questions to answer, and this input is extremely valuable for continued research and development.



The screenshot shows the 'Step 4: Notes and feedback' window of the EWT GUI. The window title is 'EWT GUI (cases/20180314153926)'. The interface includes a progress bar at the top with four steps: 'Case name', 'Step 1: Import chat logs', 'Step 2: Process chat logs', 'Step 3: View results', and 'Step 4: Notes and feedback'. The main content area contains the following elements:

- A dropdown menu for 'Is this an active investigation?' with 'Historic police case' selected.
- A prompt: 'Please rate the following questions from strongly disagree to strongly agree:'
- Two Likert scale questions:
 - 'EWT helped to discover/find evidence' with radio buttons for 'Strongly disagree', 'Disagree', 'Neutral', 'Agree', and 'Strongly agree'. The 'Strongly agree' option is selected.
 - 'EWT provided leads or lines for enquiry for an investigation' with radio buttons for 'Strongly disagree', 'Disagree', 'Neutral', 'Agree', and 'Strongly agree'. The 'Strongly agree' option is selected.
- A text input field for 'How much time do you estimate the automated analysis saved compared to manual analysis of these chat logs?' with a 'Minutes' dropdown menu.
- A table for 'Having reviewed the results, in your own judgement which of the chatlogs were of interest?'

	Grooming	Suspicious	Chat log
34	<input type="checkbox"/>	<input type="checkbox"/>	cases/sample_data/chatlogs/Log 1.txt

Please let us know whether this is a live or historical case; whether it has (or would have) assisted the investigation; and how much time EWT saved compared to typical manual/keyword searches.

Based on the judgement of the investigator, state which files were **grooming** (that is evidence or directly relevant to the investigation) or **suspicious** (related or helpful but not directly useful as evidence).

There are just two questions where we ask for some written feedback:

Please provide some written feedback, with any positive or negative feedback or suggestions. A sentence or two at minimum please.

Finally, whether there are any chat messages that have been incorrectly flagged or missed. The user is prompted to redact any sensitive content (such as names and places) and provide some examples.

The program saves these feedback responses along with redacted versions of the analysis outputs to a "feedback" folder. The redacted versions do not contain any message

contents or participant names. We ask that the feedback folder be provided back to us for research purposes. Over the following months we will arrange for these to be returned to us.

This information will enable us to evaluate and improve the system, and develop further techniques to automate via machine learning the process of flagging chat logs most likely to contain grooming.

Information sheet

Project aims

Thank you for your participation in this study. The aim of this work is the creation of tools and techniques to detect and flag evidence of predatory behaviour by scanning chat and other social media logs extracted from seized equipment. Although the research literature proposes techniques for modelling and detecting “luring” dialogues (Olson et al., 2007; Leatherman, 2009), Digital Forensics Units (DFU) typically rely on manual review, searching, and simple keyword lists. Based on analysis of this information and the associated academic papers, a series of predatory speech acts were identified as being relevant to the automated detection of grooming. The EWT scanning algorithm was tuned and refined first against PJ logs and also against real world data.

The result is a software tool that can be used by investigators to automate log-file screening to quickly filter through chat logs to identify evidence. The approach is sufficiently generic to allow the same tool to be used with different lexicons to detect other dialogues of concern such as cyber-stalking and radicalisation or terrorist recruitment.

Current status: we are piloting the software in a number of forces (started May 2018). UK forces are invited to contact DCI Vanessa Smith (vanessa.smith@westyorkshire.pnn.police.uk) and Dr Z. Cliffe Schreuders (c.schreuders@leedsbeckett.ac.uk) to join the pilot.

The results from this pilot will help us to evaluate our existing approach, and to continue research and development into techniques for digital investigation and detection of predatory behaviour.

Your participation

You have been chosen to take part in this study, because you are involved in police cases and processes that can potentially involve digital evidence and cybercrime, processing chat logs for predatory behaviour as part of police investigations.

Your input is very valuable to the project, and we hope you will continue to participate. However, you are under no obligation to take part and can withdraw involvement at any stage.

What do I have to do?

Forces who participate in the pilot will use the EWT software to triage chat logs as part of digital investigations, and provide feedback on the effectiveness of the approach. Forces can choose to trial the software on historical cases, or deploy onto live cases, as they deem fit, in combination with any tools and techniques they traditionally use.

The identity of investigators, victims, and offenders

We ask police to ensure the information they provide via the feedback survey contains no

sensitive data, including their own identity.

The feedback data set sent back to us should include no sensitive data; the software automatically creates two copies of its output, a sensitive version for police use (including message contents and participants names), and a redacted version for research purposes. Forces are welcome to review the raw data and software code before the feedback directory is sent to us for analysis.

No sensitive personally identifiable data will be published. Results are normally presented in terms of groups of individuals, and overall statistics and findings.

What are the benefits of taking part?

As a force engaged in the pilot, you will have free access to the EWT software (and you can continue using this software for free after the pilot). The EWT software is intended to provide you with tools to save time and increase the effectiveness of digital investigations involving large quantities of chat logs.

You will be helping us to identify areas for improvement for yourselves in your day-to-day roles. These results will be used to understand how these tools can be improved, and we will use this information to continue development of these techniques and software, potentially impacting your own working environment and the effectiveness of cybercrime investigation.

This work is also intended to benefit other police forces and researchers: results will be published in academic venues, such as peer-reviewed conferences and journals. Results will also be summarised and disseminated in presentations, on websites, and in training materials.

Who is funding the research?

Development of EWT was supported by a Police Knowledge Fund grant, administered by the Home Office, College of Policing, and the Higher Education Funding Council for England (HEFCE). Leeds Beckett University and West Yorkshire Police led the CARI Project and are continuing to collaborate on the research.

CARI Project overview

The CARI Project is a large-scale collaboration between West Yorkshire Police and the Cybercrime and Security Innovation Centre (CSI Centre) at Leeds Beckett University. The CARI Project aims to improve and incorporate an evidence-based approach into the policing of digital forensics and cybercrime investigations. An extensive needs assessment of UK policing and cybercrime and digital evidence was conducted to understand the current situation, and to identify needs across the force. The CARI Project also involved implementing a training and research programme that has directly impacted the capability of the digital forensics and cyber units within West Yorkshire Police to engage in research. This needs assessment and research training led to the development of a set of research

proposals, which were scored and selected. Subsequently, academics and police staff co-produced 9 research and development workstreams: a framework for seizure, preservation and preservation of cloud evidence; automated forensic analysis; image linkage for victim identification and framework for image fingerprint management; automated grooming detection; frontline officer awareness development and decision support mobile app; assessment of methods of cyber training; an evaluation of the role of the Digital Media Investigator within WYP; and characteristics of victims of cybercrime. Each of these projects were designed to address needs within law enforcement and outputs include evidence-based procedures, new capabilities such as software/algorithms, and actionable intelligence.

Consent statement

By participating in the EWT pilot and completing the feedback surveys:

I confirm that I have read and understand the above.

I understand that all personal information will remain confidential and that all efforts will be made to ensure I cannot be identified (except as might be required by law).

I agree that data gathered in this study may be stored anonymously and securely, and may be used for future research.

I understand that my participation is voluntary and that I am free to withdraw at any time without giving a reason.

I agree to take part in this study.