Named Entity Recognition for Drone Forensic Using BERT and DistilBERT

Swardiantara Silalahi
Department of Informatics
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
6025211018@mhs.its.ac.id

Tohari Ahmad
Department of Informatics
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
tohari@if.its.ac.id

Hudan Studiawan
Department of Informatics
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
hudan@its.ac.id

2022 International Conference on Data Science and Its Applications (ICoDSA) | 978-1-6654-8665-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICoDSA55874.2022.9862916

***Abstract*—The increase in UAV usage and popularity in many fields opens new opportunities and challenges. Many business sectors are benefiting from the UAV device employment. The wide range of drone implementation is varied, from business purposes to crime. Hence, further mechanisms are needed to deal with drone crime and attacks both administratively and technically. From a technical view, the security protocol is needed to keep the drone safe from various logical or physical attacks. In case a drone experiences incidents, a forensic protocol is needed to perform analysis and investigation to uncover the incident, understand the attack behavior, and mitigate the incident risk. Among the existing drone forensic research efforts, there is limited attempt to utilize specific drone artifacts to perform forensic analysis. Therefore, this paper investigates the potential of NER (Named Entity Recognition) as an initial step to perform information extraction from drone flight logs data. We use Transformers-based techniques to perform NER and assist the forensic investigation. BERT and DistilBERT pre-trained models are fine-tuned using the annotated data and get the F1 scores of 98.63% and of 95.9%, respectively.**

Keywords—drone forensic, named entity recognition, transformers neural network, network infrastructure, BERT, DistilBERT

I. INTRODUCTION

In this modern era, human life cannot be separated from the role of technology. The use of technology has been widely used and adopted in almost all aspects of life. Big companies and businesses utilize the advancement of technology to optimize and regulate the business process. One of the emerging technologies lately is IoT (Internet of Things). Among all the popular IoT devices, the drone, which is called flying IoT, is considered one of the most used in the future. The number of consumer drone shipments globally has reached around 5 million units in 2020 and is expected to increase to 9.6 million consumer drone shipments globally in 2030 [1]. A consumer drone is a type of civilian multi-purpose drone used for recreational purposes such as capturing photographs and recording videos for fun [2].

The increase in drone usage in many fields opened new challenges in securing this device. Other than the civilian multi-purpose drone, there are three other types of drones based on the purpose, which are terrorist, criminal, and military drones [2]. For these types of drones, failure and error are not tolerated as much as in consumer drones. Therefore, it is important to ensure the security of drone devices. For this reason, it is important to develop more advanced security and forensic techniques to deal with the attacks against drone devices [3].

There are two types of drone attacks, i.e., physical, and logical attacks. Logical attack, commonly called cyber-attack, includes infection, exploitation, information gathering, interception, authentication, and jamming [2]. These attack types target different aspects of drone security: privacy, integrity, availability, and data confidentiality. Drone device has several vulnerabilities and threats, such as prone to spoofing, malware infection, data interference and interception, manipulation, technical issues, operational issues, natural issues, and Wi-Fi jamming. Several existing cyber-countermeasures for these attacks are rule-based and signature-based IDS, anomaly-based detection, drone communication encryption, and stored data encryption [2].

Other than preventive actions, as previously mentioned, a forensic investigation also needs to be performed upon an incident to understand more about the attack's behavior and how to mitigate the risk caused by the incident [4]. In the existing drone forensic framework, as proposed in [3], there are four phases of the investigation process: pre-incident preparation, post-incident preparation, data acquisition, and data analysis. This research focuses on the data analysis phase, which utilizes forensic evidence to conduct analysis and answer the forensic objectives.

The existing drone forensic evidence analysis research comprises timeline construction, memory analysis, event correlation, radiofrequency analysis, and evidence identification [3]. Another research performing drone data analysis is for visualizing the route taken by the aircraft and extracting metadata such as owner username, smartphone controller OS, sensor, and battery information [5]. Utilizing the radio-control signals makes it possible to identify the drone pilot information [6].

To the best of our knowledge, among the existing research in the data analysis phase of the drone forensic investigation framework, no study utilizes log messages in the flight log data to conduct a forensic investigation. Therefore, as the main contribution of this paper, a Drone Named Entity Recognition (DroNER) model using Bidirectional Encoder Representation from Transformers (BERT) and DistilBERT is proposed. Another contribution of this paper includes the annotated flight log data and the identified entity types in the drone forensic domain.

This paper consists of five sections. The remainder of this paper's structure is as follows. Section II discusses several related published research and explains the position of this research. Section III explains the research methods and the proposed model. The experimental results and analysis are provided in Section IV. Section V concludes the research and delivers the research limitation and future works.

Authorized licensed use limited to: Malaviya National Institute of Technology Jaipur. Downloaded on October 21,2023 at 01:36:40 UTC from IEEE Xplore. Restrictions apply.

II. Related Works

A. Drone Forensic

Drone forensics is a relatively new research area. The development and advancement of Unmanned Aerial Vehicle (UAV) technology bring this topic to the surface and interest the researchers. The most common research in drone forensics is based on a case study. This kind of research performs a forensic investigation against a conditioned incident or scenario. The end-to-end process from the data acquisition phase until the incident report. Yousef et al. [7] propose a set of procedures to guide the forensic investigator when performing an investigation against the DJI Mavic Air drone model. Several tools are used to acquire the evidence and explain the successfully obtained data, which potentially help the investigation process. Another similar research was conducted against DJI Phantom [8], DJI Spark [9], and the Yuneec Typhoon model [10]. The case studies conclude that the controller device of the drone contains much helpful information that makes the correlation analysis between the UAV and the mobile application feasible by comparing the artifacts. Some research also proposed a technical process for drone forensic investigation. As in [10], ten steps must be followed to perform an end-to-end analysis from preparation to report findings.

One of the data acquisition phase challenges is analyzing the encrypted files. Encrypted evidence data is standard for DJI models. Although DJI provides the decryptor application, there is a condition where the data needs to be decrypted without DJI proprietary apps. Therefore, some research proposed tools to assist the investigator in performing analysis. Clark et al. [11] propose DROP (Drone Open-source Parser), a tool to parse the .DAT files and decrypt the payload data contained by the .DAT files. This tool can also perform correlation analysis between the .DAT file and the .TXT flight log file. While the data flash and telemetry log analysis can be done using GRYPHON [12]. Since the data flash log stores the recorded events during the flight, the tool can perform timeline analysis, extract flight data to find an anomaly, GPS coordinates mapping, and many more functionalities. To help the forensic investigator find the most appropriate tools, Viswanathan et al. [13] study the available tools, while Salamh et al. [14] perform a case study to review the functionality of available tools that have been discovered.

Before starting a forensic investigation, it is important to understand the drone device and its components [15]. Therefore, Jain et al. [15] propose a framework consisting of 12 steps. The first five steps are used to identify and verify the sensor and data of the drone device. A more comprehensive framework offered by [3] consists of four investigation phases. However, the data analysis phase still covers the general potential topic such as integrity check, timeline construction, and evidence identification. There are still few studies that focus on analyzing one type of drone forensic data.

Drone forensic research is dominated by case studies and tools proposal and evaluation. There are several surveys and systematic reviews [3][16]. The number of research conducting analyses against specific types of drone data is still limited. Therefore, this paper is trying to fill the research gap by exploring how to perform information extraction from flight logs. The extracted information is expected to assist the forensic investigator in focusing directly on the related information in the flight logs regarding an incident.

B. Cybersecurity Named Entity Recognition

NER plays an important part in general Natural Language Processing (NLP) research and domain-specific problems. The ability of NER to extract some useful information in text data can help the information extraction process faster and more accurately. This is done by seeing and recognizing tokens that potentially belong to a particular type of entity [16]. Especially in the cybersecurity domain, much useful information is stored in system logs and written in a less human-readable format. It will be a labor-intensive activity to perform manual analysis. Since the records are text data, researchers employ NLP techniques to process and analyze the text data automatically.

The complexities of cybersecurity data have been one of the main challenges to face. Several systems and devices have different formats of logs. There is no standardized naming convention containing many abbreviations, technical terms, use of conjunction often, and massive nesting [17].

The previous state-of-the-art of cybersecurity NER was proposed by Ma et al. [18], who used XBiLSTM-CRF architecture to perform NER with a public cybersecurity dataset. The idea of concatenating the vector representation of a word with the output of the bidirectional Long Short-Term Memory (LSTM) layer can improve the model's performance. To decoding the concatenated output, the Conditional Random Field (CRF) layer is employed as it can learn the relation between the labels in a sequence.

Working with deep learning models requires most of the effort focusing on how to provide decent input representations. This input representation is commonly learned by word embedding methods such as GloVe [19], Word2vec [20], BERT, and ELMo [21]. GloVe uses global statistics to extract the semantics of a word, while ELMo and BERT can extract contextualized vector representation. Gao et al. [22] develop a domain knowledge and data-driven NER system by providing a companion representation of the word embedding vectors and employing an attention mechanism to assign higher weights to relevant information in a sequence. The experiment shows that the proposed model can recognize rare entities better.

Further development of the NER system in cybersecurity employing BERT is proposed in [23]. Whole Word Mask is used instead of the random partial masking as used in BERT. This masking method can deal with cybersecurity data better because the masking is performed for the whole word, instead of at a word piece level. This method solved one of the challenges in cybersecurity NER, which is the frequent use of conjunction in a word such as "buffer-overflow" or "man-in-the-middle attack".

III. Methodology

A. Data Collection and Extraction

The data used in this research were taken from the publicly available drone dataset provided by VTO Labs[1]. There are 82 drone data from 31 different drone models. For initial research, this paper used 18 drone data from 7 different

[1] https://www.vtolabs.com/drone-forensics/

Authorized licensed use limited to: Malaviya National Institute of Technology Jaipur. Downloaded on October 21,2023 at 01:36:40 UTC from IEEE Xplore. Restrictions apply.

drone models, as shown in Table I. We choose the selected drone data because they are from the same make, i.e., DJI. For every drone data, there are several sources such as external SD Card, internal SD Card, Android controllers, and iOS controllers. These four different sources store different data in different structures. In this paper, only human-readable log data will be used. This kind of data can be found in flight logs. To get the flight logs, the log data from iOS and android controller devices were extracted using Autopsy[2] and DJI Phantom Log Viewer[3], respectively. The extracted logs were then analyzed to understand the structure of the logs and find the human-readable messages. The extracted log messages are then collected to form a corpus for further processing steps.

B. NER for Information Extraction

Analyzing text data using NLP methods is one of the emerging topics nowadays. This technique can be adapted to numerous domain applications. For the forensic domain, the NLP method can be used to extract information within the text data of the evidence. Named Entity Recognition as one of the NLP methods can be used as a preprocessing component to perform certain downstream NLP tasks [24] or as an initial step in conducting an information extraction process [25]. The unstructured characteristic of text data requires a more complex analysis process than structured data, even though most of the data available are in the unstructured format. In the general domain, NER is used to extract useful information such as organization, person, or location names contained in a sentence or document. In a domain-specific problem, the named entities will be completely different. As in the agriculture domain, the named entities comprise food, farm, climate, disease, and temperature [25].

NER can be seen as an initial step to performing aspect-based sentiment analysis. As in [26], the log message can be considered as the aspect of the sentiment, which then needs to be analyzed further to classify the sentiment. NER is employed as the method to parse and extract the log message. This paper utilizes the power of NER to extract important information in text data to assist the investigator in carrying out forensic investigations of drone devices.

C. DistilBERT for Named Entity Recognition

The use of a pre-trained language model has a huge impact on NLP research. Language models trained using large text data are considered valuable and helpful in performing downstream NLP tasks such as text classification, token classification, text generation, and others. BERT [27] is one of the pre-trained language models trained using BookCorpus, which contains 800M words, English Wikipedia, which contains 2,500M words, 30,000 tokens vocabulary, and WordPiece tokenization as proposed by Wu et al. [28]. The architecture of the Transformer's Encoder will not be discussed in this paper since it is clearly explained in the original paper [29].

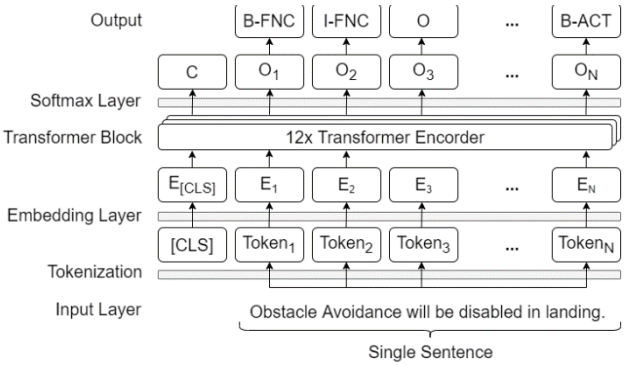

Fig. 1 BERT architecture for NER.

TABLE I. DRONE FLIGHT LOG MESSAGE DATA SOURCE

Drone Model	Drone Identifier	Num. of Message
DJI Inspire 1	DF010	48
	DF011	7
DJI Inspire 2	DF025	17
	DF026	16
	DF027	234
DJI Matrice 600	DF034	87
DJI Mavie 2	DF067dd	5
	DF068	32
	DF069	5
DJI Mavie 2 Enterprise	DF080	18
	DF081	27
	DF082	25
DJI Mavie Air	DF048	25
	DF049	0
	DF050	66
DJI Mavie Pro	DF019	28
	DF020	26
	DF021	6

BERT training process can be decomposed into two phases, pre-training, and fine-tuning. BERT is pre-trained using two unsupervised tasks, Masked Language Model (MLM) and Next Sentence Prediction (NSP). For the MLM task, it masks a portion of the input tokens randomly and then predicts the masked tokens. This is done to preserve the bidirectional nature of BERT. The NSP task is chosen for the reason of accommodating the downstream tasks, which incorporate two different sentences such as Question Answering (QA) and Natural Language Inference (NLI).

In this paper, the fine-tuning step is used to perform a downstream task using DistilBERT, which is Named Entity Recognition. DistilBERT is a light version of BERT, which is pre-trained using only the MLM task but with the same corpus. DistilBERT is 40% smaller than BERT in size, 60% faster, and retains 97% of BERT performance. It makes DistilBERT feasible to be implemented in a device with limited computation resources [30], like a drone. The pre-trained contextual word embedding from DistilBERT will be used to represent the input tokens into vectors. A dense layer is put on top of the DistilBERT with softmax activation function to interpret the computation results. The resulted output will be a d dimensional vector of the probability of the label, where d is the number of labels. The architecture of the model is shown in Fig. 1.

[2] https://www.autopsy.com/

[3] https://www.phantomhelp.com/logviewer/upload/

Authorized licensed use limited to: Malaviya National Institute of Technology Jaipur. Downloaded on October 21,2023 at 01:36:40 UTC from IEEE Xplore. Restrictions apply.

D. Fine-tuning DistilBERT

To get the best model, hyperparameter tuning is performed by following the recommendation from the BERT original paper [24]. The space of the parameter search is shown in Table III. We experiment with several additional alternatives for the learning rate since the recommended learning rate results in a sub-optimal model. We also study the effect of using cased and uncased tokenizers.

NER is one of the multiclass classification problems. Since the data composition between the classes is imbalanced, the accuracy score cannot be used to represent the actual model performance. The recognition of the labels with the smaller number of data is rewarded disproportionally. The F1-Score is used as the standard metric to evaluate the model with a class imbalance problem by computing the harmonic average between the precision and recall. The F1 score is computed using the following equation for the binary classification.

TABLE II. ENTITY TYPE SAMPLE

Word	Entity Type	Tag
Taking	Action	B-ACT
Off	Action	I-ACT
Landing	Component	B-CMP
Gear	Component	I-CMP
Obstacle	Function	B-FNC
Avoidance	Function	I-FNC
Low	Issue	B-ISS
Power	Issue	I-ISS
Sport	State	B-STE
Mode	State	I-STE

TABLE III. NUM. OF TOKEN FOR EACH ENTITY TYPE

Dataset	Component	Action	State	Function	Issue
Train	121	128	91	259	107
Test	55	49	27	110	37
Total	176	177	118	369	144

$$F1 = \frac{2 \times precision \times recall}{precision + recall} \quad (1)$$

It is different from the multiclass classification problem. There are two approaches to computing the F1 score, either using macro average or micro average. In this research, the micro average is used. Given TP_A, FP_A, and FN_A are the number of True Positive, False Positive and False Negative of class A, respectively. Then, the Precision score of class A (P_A) will be:

$$P_A = \frac{TP_A}{TP_A + FP_A} \quad (2)$$

and Recall score of class A (R_A) will be:

$$R_A = \frac{TP_A}{TP_A + FN_A} \quad (3)$$

Therefore, the F1 score of class A will be:

$$F1_A = \frac{TP_A}{TP_A + \frac{1}{2}(FP_A + FN_A)} \quad (4)$$

Consider we have $N = \{A, \ldots, N\}$ number of classes. The micro-average F1 score can be computed using the below formula.

$$F1 = \frac{\sum_A^N \quad TP_A}{\sum_A^N \quad TP_A + \frac{1}{2}(\sum_A^N \quad FP_A + \sum_A^N \quad FN_A)} \quad (5)$$

While for the macro-average, we simply take the average of F1 socre of class A until class N.

$$F1 = \frac{\sum_A^N \quad F1_A}{N} \quad (6)$$

TABLE IV. HYPERPARAMETER SEARCH SPACE

Hyperparameter	Value
Epoch	2, 3, 4
Learning Rate	1e-4, 2e-5, 3e-5, 5e-5
Batch Size	16, 32

TABLE V. DATA COMPOSITION

Dataset	Sentence	Token	Entity
Train	470	2660	706
Test	202	1018	278
Total	672	3678	984

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experiment conducted in this research consists of five steps, i.e., data extraction, entity identification, data annotation, model fine-tuning, and model evaluation. The steps are shown in Fig. 2.

A. Data Understanding and Annotation

This paper is the first research in the drone forensic domain that employs NER to the best of our knowledge. For this reason, there is no annotated data available yet. In order to produce well-annotated data, the entity types in the drone forensic domain need to be identified first. The identification process of entity types in drone flight logs is the second step of this research after extracting and collecting the flight log data. This process includes unique message filtering, reading the unique message one by one, and extracting words or phrases that potentially belong to particular entity types. The identified entity types will be used as a reference to perform annotation. Table II shows the sample of identified entity types, and Table III shows the number of tokens for each entity type. The reason for choosing the entity types mentioned in the table is that those entities are assumed to have a strong relationship with certain drone incidents. For example, a message containing "Low Power" phrase strongly

Authorized licensed use limited to: Malaviya National Institute of Technology Jaipur. Downloaded on October 21,2023 at 01:36:40 UTC from IEEE Xplore. Restrictions apply.

relates to the aircraft's condition of losing power immediately.

The IOB scheme is one of the commonly used annotation schemes to perform data annotation in NER research. It has been adopted by the CoNLL [31]. By using this scheme, each word in a sentence will be assigned either the beginning (B), inside (I), or outside(O) tag. A word is assigned with a beginning (B) tag means the word is the beginning of a known entity. Suppose this word is followed by a consecutive word with the same known entity type; the word will be assigned the inside (I) tag. Other than that, it will be labeled as outside (O). The number of sentences, tokens and entities resulting from the annotation process is shown in Table V. The result of the manually annotated data follows the CoNLL format. For reproducibility, we made the dataset accessible through the Hugging Face platform[4], and the experiment code on Github[5].

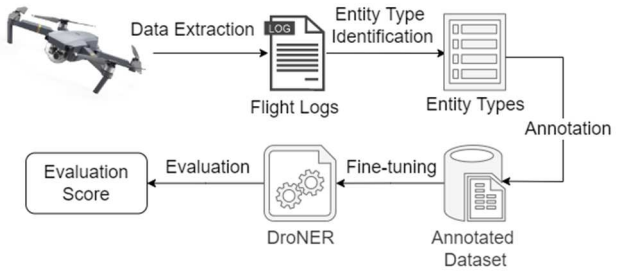

Fig. 2 Experimental design.

The dataset used in this research is originally from the extraction process without removing the duplicate messages since not many messages are contained in the drone controller device. The dataset is split 70% for training and 30% for evaluation. The composition of the dataset is shown in Table. V. For an initial result, we avoid the labeled data having polysemous words.

B. DistilBERT Hyperparameter Tuning

Since DistilBERT is a general pre-trained model, it needs to be fine-tuned in order to perform a downstream task, which is NER in this case. DistilBERT base is used in this research since the dataset is relatively small. DistilBERT base consists of transformer encoder blocks, hidden size, and self-attention heads with total parameters of 66M [30]. For the tokenizer, distilbert-base-cased is chosen since the entity commonly uses the capital case as in city, organization, and person names. This also happens in the drone flight logs data. Many words which belong to certain entity types are written in a capital case. After experimenting using cased and uncased input tokenizers, we can conclude that using case-sensitive input tokenization is beneficial for a NER model. The use of case insensitive input tokenizer decreases the model's performance by more than 50%.

As recommended in the original paper of BERT, the hyperparameters search based on the reference in Table IV resulting the eight best models as shown in Table VI. The effect of batch size is not significantly affecting the model's performance. Instead, it is affecting the training time. Since the data size is small, the training duration is relatively the same. The relation between learning rate and epoch is quite strong in the opposite direction. If we increase the learning rate, we need to reduce the number of epochs, and vice versa. If we increase both the learning rate and epoch number, the model potentially surpasses the convergence point. What if we decrease both the learning rate and the number of epochs? Turns out the model will be at a sub-optimal point.

Since this is initial research in drone forensics incorporating NER as the method, there is no significant modification in the BERT architecture. This research aims to see the prospective of NER in the drone forensic domain.

C. Evaluation Results

The NER model resulted from fine-tuning BERT, and DistilBERT can perform well. It can be seen from the F1 score of more than 90% for most of the model's parameters configuration. Since the performance scores are slightly different, we investigate the resulted model size. For BERT, the approximate size is around 430MB. Significantly different, the DistilBERT only resulted in a 260MB model size. Considering drone devices have limited computation resources, DistilBERT will likely be the suitable model to be choosen to assist forensic investigators in spotting the region of interest in the drone flight log data.

NER is sensitive to polysemous words. For this reason, the annotation process avoids the label having polysemous words to get an initial result. It turns out that the models perform well without polysemous words. The Traditional NER system needs an additional step called entity disambiguation to deal with polysemous words. Since the Transformers model can learn from the context of a sentence, we plan to further analyze the effect of polysemous words in the dataset and see if the model can recognize the words in a different context as different entities.

V. CONCLUSION

More and more pre-trained Language Models available cause less effort to perform NLP downstream tasks. This research utilizes the available pre-trained Language Model, BERT, and DistilBERT to build a Drone Named Entity Recognition (DroNER) system. A publicly available drone dataset from VTO Labs is extracted to build the NER dataset using the IOB annotation scheme. A hyperparameter search is performed in the fine-tuning process to get the model with the best performance. The presented models perform well as demonstrated by the F1 score of 98.63% and of 95.9% for BERT and DistilBERT, respectively. The obtained results are good because of the consistency of the labeling, which means that our dataset contains no polysemous words.

For the future experiment, we plan to analyze the effect of polysemous words on the model's performance. This research can be considered as an initial step in performing further NLP applications in the drone forensic domain, such as aspect-based sentiment analysis. The recognized entity types could be considered as the sentiment aspect in a sentence or document. The extracted entity could also be linked to a knowledge base to assist the investigator in understanding technical terms and domain-specific abbreviations. Therefore, it can reduce the time consumed in forensic analysis activity.

[4] https://huggingface.co/datasets/swardiantara/drone-ner

[5] https://github.com/swardiantara/droner

Authorized licensed use limited to: Malaviya National Institute of Technology Jaipur. Downloaded on October 21,2023 at 01:36:40 UTC from IEEE Xplore. Restrictions apply.

TABLE VI. MODEL'S HYPERPARAMETER TUNING

Model Type	Batch Size	Epoch	Learning Rate	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	Train Time (s)
Bert-base-cased	32	4	1.00E+04	98.723	97.297	98.182	97.738	507
	32	3	1.00E+04	98.821	95.495	96.364	95.928	384
	16	3	1.00E+04	98.527	97.273	97.273	97.273	398
	16	**4**	**1.00E+04**	**99.018**	**99.083**	**98.182**	**98.630**	**530**
Distilbert-base-cased	32	4	1.00E+04	94.619	94.619	95.909	95.260	258
	32	3	1.00E+04	95.023	95.023	95.455	95.238	193
	16	4	1.00E+04	94.619	94.619	95.909	95.260	276
	16	**3**	**1.00E+04**	**95.527**	**95.909**	**95.909**	**95.909**	**207**

REFERENCES

[1] F. Laricchia, "Consumer drone unit shipments worldwide from 2020 to 2030," *Statista*, 2022. https://www.statista.com/statistics/1234658/worldwide-consumer-drone-unit-shipments.

[2] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, 2020.

[3] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, "Research Challenges and Opportunities in Drone Forensics Models," *Electronics*, vol. 10, no. 13, 2021.

[4] F. Iqbal *et al.*, "Drone forensics: Examination and analysis," *Int. J. Electron. Secur. Digit. Forensics*, vol. 11, no. 3, pp. 245–264, 2019.

[5] M. Yousef, F. Iqbal, and M. Hussain, "Drone Forensics: A Detailed Analysis of Emerging DJI Models," in *2020 11th International Conference on Information and Communication Systems (ICICS)*, pp. 66–71, 2020.

[6] A. Shoufan, H. M. Al-Angari, M. F. A. Sheikh, and E. Damiani, "Drone Pilot Identification by Classifying Radio-Control Signals," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 10, pp. 2439–2447, 2018.

[7] M. Yousef and F. Iqbal, "Drone Forensics: A Case Study on a DJI Mavic Air," in *16th International Conference on Computer Systems and Applications (AICCSA)*, 2019.

[8] T. E. A. Barton and M. A. Hannan Bin Azhar, "Forensic analysis of popular UAV systems," in *2017 Seventh International Conference on Emerging Security Technologies (EST)*, 2017.

[9] D.-Y. Kao, M.-C. Chen, W.-Y. Wu, J.-S. Lin, C.-H. Chen, and F. Tsai, "Drone Forensic Investigation: DJI Spark Drone as A Case Study," *Procedia Comput. Sci.*, vol. 159, pp. 1890–1899, 2019.

[10] F. E. Salamh, U. Karabiyik, and M. K. Rogers, "RPAS Forensic Validation Analysis Towards a Technical Investigation Process: A Case Study of Yuneec Typhoon H," *Sensors*, vol. 19, no. 15, 2019.

[11] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," *Digit. Investig.*, vol. 22, pp. S3–S14, 2017.

[12] E. Mantas and C. Patsakis, "GRYPHON: Drone Forensics in Dataflash and Telemetry Logs," in *Advances in Information and Computer Security*, 2019.

[13] S. Viswanathan and Z. Baig, "Digital Forensics for Drones: A Study of Tools and Techniques," in *Applications and Techniques in Information Security*, 2020.

[14] F. E. Salamh, M. M. Mirza, and U. Karabiyik, "Uav forensic analysis and software tools assessment: Dji phantom 4 and matrice 210 as case studies," *Electron.*, vol. 10, no. 6, pp. 1–14, 2021.

[15] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," in *2017 IEEE Sensors Applications Symposium (SAS)*, 2017, pp. 1–6, 2017.

[16] T. M. Georgescu, B. Iancu, A. Zamfiroiu, M. Doinea, C. E. Boja, and C. Cartas, "A survey on named entity recognition solutions applied for cybersecurity-related text processing," *Adv. Intell. Syst. Comput.*, vol. 1184, pp. 316–325, 2021.

[17] C. Gao, X. Zhang, M. Han, and H. Liu, "A review on cyber security named entity recognition," *Front. Inf. Technol. Electron. Eng.*, vol. 22, no. 9, pp. 1153–1168, 2021.

[18] P. Ma, B. Jiang, Z. Lu, N. Li, and Z. Jiang, "Cybersecurity named entity recognition using bidirectional long short-term memory with conditional random fields," *Tsinghua Sci. Technol.*, vol. 26, no. 3, pp. 259–265, 2021.

[19] J. Pennington, R. Socher, and C. Manning, "Glove: Global Vectors for Word Representation," in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, vol. 19, no. 5, pp. 1532–1543, 2014.

[20] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient Estimation of Word Representations in Vector Space," *1st Int. Conf. Learn. Represent. ICLR 2013 - Work. Track Proc.*, pp. 1–12, Jan. 2013.

[21] M. Peters *et al.*, "Deep Contextualized Word Representations," in *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers)*, pp. 2227–2237, Feb. 2018.

[22] C. Gao, X. Zhang, and H. Liu, "Data and knowledge-driven named entity recognition for cyber security," *Cybersecurity*, vol. 4, no. 1, p. 9, May 2021.

[23] S. Zhou, J. Liu, X. Zhong, and W. Zhao, "Named Entity Recognition Using BERT with Whole World Masking in Cybersecurity Domain," in *2021 IEEE 6th International Conference on Big Data Analytics (ICBDA)*, pp. 316–320, 2021.

[24] J. Li, A. Sun, J. Han, and C. Li, "A Survey on Deep Learning for Named Entity Recognition," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 1, pp. 50–70, 2022.

[25] Q. H. Ngo, T. Kechadi, and N.-A. Le-Khac, "Domain Specific Entity Recognition With Semantic-Based Deep Learning Approach," *IEEE Access*, vol. 9, pp. 152892–152902, 2021.

[26] H. Studiawan, F. Sohel, and C. Payne, "Anomaly Detection in Operating System Logs with Deep Learning-Based Sentiment Analysis," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 5, pp. 2136–2148, 2021.

[27] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Minneapolis, MN, USA, June 2-7, Volume 1*, 2019, pp. 4171–4186, 2019.

[28] Y. Wu *et al.*, "Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation," *CoRR*, vol. abs/1609.08144, 2016, [Online]. Available: http://arxiv.org/abs/1609.08144.

[29] A. Vaswani *et al.*, "Attention Is All You Need," *CoRR*, vol. abs/1706.03762, 2017, [Online]. Available: http://arxiv.org/abs/1706.03762.

[30] V. Sanh, L. Debut, J. Chaumond, and T. Wolf, "DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter," *CoRR*, vol. abs/1910.01108, 2019, [Online]. Available: http://arxiv.org/abs/1910.01108.

[31] N. Alshammari and S. Alanazi, "The impact of using different annotation schemes on named entity recognition," *Egypt. Informatics J.*, vol. 22, no. 3, pp. 295–302, 2021.

Authorized licensed use limited to: Malaviya National Institute of Technology Jaipur. Downloaded on October 21,2023 at 01:36:40 UTC from IEEE Xplore. Restrictions apply.