Automatically Unaware: Using Data Analytics to Detect Physiological Markers of Cybercrime

Nancy Mogire[1(✉)], Randall K. Minas[2], and Martha E. Crosby[1]

[1] Information and Computer Sciences, University of Hawaii at Manoa, POST 317 1680 East-West Road, Honolulu, HI 96822, USA
nmogire@hawaii.edu

[2] Shidler College of Business, University of Hawaii at Manoa, 2404 Maile Way Suite E601f, Honolulu, HI 96822, USA
rminas@hawaii.edu

Abstract. Cybercrime investigation is reliant on availability of adequate and valid digital artifacts useable for reconstructing security incidents or triangulating other available information to make it useful. Various operational artifacts of computer systems, networks and software have been studied and gradually applied as forensic evidence. However the scope of studies on human-generated artifacts as forensic evidence has been limited mostly focusing on surveillance images, with DNA deposits being widely studied via older forensic fields. We present the case that further focus on human-centric evidence in form of physiological measurements is useful in triangulating other evidence as well as in making some direct inferences. In this concept paper: we pair electroencephalography (EEG) with change point detection algorithms to conceptually model the acquisition and processing of EEG signals into forensic artifacts; propose continuous data reduction and packaging to keep the system forensic-ready; suggest a schema for validating such artifacts towards their applicability as forensic evidence; and model a study to be used in testing the conceptual model. This work contributes to cybersecurity research by highlighting human-generated artifacts as a forensic big data resource and presenting a methodology for harnessing the data to turn it into useful information.

Keywords: Digital forensics · Forensics artifacts · Physiological measures Electroencephalography · Cybersecurity

1 Introduction

CYBERCRIME, crimes that are committed electronically, take various forms. Often, the computer is either a tool or a target. The two aspects have sometimes been categorized broadly as computer-enabled and computer-dependent crimes [1]. The increase in cybercrime over the past decades has been staggering, including increased financial scams, child pornography, illegal gambling, cyber bullying, espionage, system vandalism using viruses and election interference [2]. The proliferation of cybercrime over the years led to the growth of computer forensics as a new forensic field.

Forensics involves acquisition and analysis of relevant data for application as evidence in legal or civil cases. There are many informational artifacts in networks

D. D. Schmorrow and C. M. Fidopiastis (Eds.): AC 2018, LNAI 10915, pp. 316–328, 2018.
https://doi.org/10.1007/978-3-319-91470-1_26

including network activity metadata, system status and usage details as well as software activity data. However, there is also seemingly untapped data from the human component of the computing system. Some of this has been utilized (e.g., DNA and camera footage), yet the power of psychophysiological data of individuals has remained largely unexplored in forensics.

There are many forms of psychophysiological data, including skin conductance, heart rate, and eye movement data. These forms of psychophysiology have been used in the forensics field for years, but have not been used extensively to detect computer crimes. In addition, electroencephalography (EEG) provides electrical data present at the scalp that elucidates aspects of cognition and emotion. These physiological measures have been unharnessed in their ability to provide large data sets through which forensics of computer-based crimes might be detected. The power of psychophysiological data is that it is difficult and often, impossible for the user to disguise their behavior as it is preconscious.

Building off Kahneman's research [3]. System 1 is the unconscious automatic cognition that is immediate and reactive, making decisions in less than a second, and System 2 is the deliberate, thoughtful process found in theories. Most researchers conclude that much human behavior is driven by System 1, with some believing that most behavior is controlled by System 1 [3, 4]. The exact amount of behavior controlled by System 1 is debatable and lies beyond the scope of this paper. However, the key point from this research is that most researchers studying dual process cognition would agree that a meaningful amount of behavior is controlled by System 1 cognition. The key takeaway is that the cybercriminal is unable to readily hide their System 1 behavior as much of it is unconscious. This provides a valuable pathway for data analytics to be combined with psychophysiological measurement to identify events related to cybercrime.

2 Background and Related Work

2.1 Digital Forensics

Digital forensics is a term often used interchangeably with computer forensics but that has evolved to cover investigation of all kinds of devices capable of storing data [5]. The term has been defined as the science of locating, extracting, and analyzing of data from different devices, for use by specialists who interpret such data for application as legal evidence [5]. The end goal is to be able to use such evidence in legal testimony that is admissible in a court of law. Such data can also be used in internal corporate investigations. Applications of evidence include attribution of actions towards suspected sources, confirming of alibis or statements, determination of intent and authentication of documents [5]. One of the key considerations in digital forensics is how to collect evidence without altering its contents so as to sustain its admissibility in court. various methods of collecting digital evidence and the attendant issues are discussed in [6].

2.2 Examples of Digital Evidence

System based evidence: This included both volatile or non-volatile data. Volatile data includes system date and time, open TCP and UDP ports and logged on users. Non-volatile data includes operating system version, user accounts and the auditing policy [6].

Network artefacts: can also be used as digital evidence. These include session information, alerts, content transmitted over networks such headers and payload in a data packet as well as network statistics e.g. how many packets are transmitted, source and destination [6].

User information stored in devices: including wearable computing, contains various artifacts such as: Paired device information, voice commands, Bluetooth packet data, text message notifications and recent tasks [7]. The authors note that some of this data requires root access to the device in order to acquire it, which in turn causes a factory reset on the device. With a factory reset, the data may not be admissible as evidence.

2.3 Evidence Acquisition

Forensic investigation can be summarized in five steps: Collection of evidence, preservation and transportation to analysis site, Identification of evidence and planning of processing, analysis of evidence, presentation via reports [5]. The focus of our work relates to the collection or acquisition stage.

Collection of evidence often involves seizure, imaging and analysis of digital media [5]. Neuner et al. [8] discuss one of the major problems of digital forensic data collection process is the need for redundancy. As they discuss, NIST SP-800-86 recommends the use of a working copy and retention of a backup copy in case data becomes tainted during analysis. These needs increase both time and storage space overhead. The solution proposed is the reduction of a working copy by removing unnecessary and duplicate files.

2.4 Anti-forensics

Anti-forensics has been defined as “Attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct” [9]. There are several anti-forensic techniques including physical destruction of devices, tampering with log files, data hiding, signature masking. However, as discussed in [5], many of them require more advanced computing knowledge. They also present various suggestions of mitigations for these anti-forensic techniques. As they discuss, another redeeming factor is that the lack of evidence is evidence itself provided the investigators can detect the absence of data that should be present. The nature of artifacts determines whether it easy or difficult to detect an absence.

2.5 Digital Forensic Readiness of a System

As Endicott-Popovsky [10] discusses, when incidents happen in networks, the organization can find itself in the dilemma between preserving the state for forensic acquisition and quickly restoring the network. If the organization is not ready for forensic data acquisition then the time and cost may be too great. In that case, the organization may choose to focus on restoring the network which may could diminish the forensic value of relevant files.

Carrier and Spafford [11] present a model for forensic readiness. Their model consists of three phases: the first one is initial readiness which entails setting up of forensic logging, developing and testing tools. The next one is the deployment which entails detection of incidents followed by systematic verification which may lead to the opening of a crime scene investigation if necessary. Following that is investigation which involves searching for evidence and reconstructing events. The final step is the presentation of the evidence and documentation.

Kazadi and Jazri [12] present another version of readiness framework: Their framework begins with risk assessment to identify the most critical data points; development of security policy for protection of software tools used in collecting evidence data and setting of quality standards regarding such tools e.g. audit schedules. The readiness phase then continues to selection of data collection software tools and other equipment such as surveillance cameras and biometric devices. The second phase involves operations decisions such as the sensor placements based on the previously assessed risks. After this point, the data is logged based on predefined rules, after which it is preserved and stored in case it is needed. The stored logs are later processed for deletion based on a preset time policy. The deletion phase involves analysis and report generation before authorized deletion.

2.6 Validating Forensic Artifacts

Palmer [13] discusses that validity of evidence must be ascertained before it can be considered judicious and reliable in a legal argument. They further discuss that validating digital evidence requires verification of the relevant parts of such evidence including how it is created, processed, stored and transferred, so as to establish a confidence level and hence a value for the inferences drawn from such evidence. If validity of such evidence cannot be established then its weight can be at best diminished and at worst negated.

Factors that can affect validity of evidence include; evidence taken out of context or misinterpreted, misleading or false evidence, failure to identify relevant errors and difficulty in reconstructing the evidence when questions are raised during the validation process [13, 14]. Boddington et al. [15] discuss that evidence validation requires a chain of proof assertions made for such evidence. For each assertion made for the validity of the evidence, a stronger negative assertion may exist in which case such evidence may be weakened. The authors give an example of an assertion <<*data was overwritten by virus scanner*>> which gets negated by: <<*file creation date is unchanged*>>. An investigator can use a checklist that is artifact-specific to run a piece

of forensic data through an assertion chain and thereby make a claim to its validity or invalidity.

2.7 Physiological Artifacts for Digital Forensics

Mobile phone swipe gestures have been considered as a source of forensic data by Mondal and Bours [16] who employ a continuous identification [CI] model to continually verify the user. They suggest that in a closed user group, apart from detecting that an unauthorised user is on the phone and locking it, the system can also attempt to identify the adversary and store the information for evidential use. They note that this may be the first application of biometric information for continuous identification [CI]. The forensic angle of their work is that they obtain the identity of the intruder and store it as evidence. As they discuss, their focus is the protection of the system which entails locking the phone as soon as an unauthorized user is detected. The forensic extent of their work is that they obtain the identity of the intruder and store it as evidence although accuracy of this process as they note is hindered by the focus on quickly locking out the impostor [16].

Other collectable physiological measurements could potentially be applicable as digital forensic artifacts. These include heart rate, skin conductance, breath count, and electroencephalograms. As an initial focus, in the next section we consider electroencephalograms for their potential applicability.

2.8 Suitability EEG as a Source of Forensic Data

Electroencephalography (also abbreviated as EEG) is the recording of the brain's electric potentials varying in time at different frequencies per second and range from a few microvolts to a few millivolts [17]. Electroencephalograms are produced as a result of the synchronous action of numerous neurons in the brain [18]. EEG measurements are recorded from scalp electrodes [19]. Nunez and Katznelson [17] discuss that EEG signals occur and are recordable without the need for any deliberate stimuli application. For the information to be applicable for a desired usage, relevant stimuli is applied and the changes are recorded as a measure of the response to the stimuli. These changes are referred to as evoked potentials [17].

EEG signals provide a unique signature and can be used to distinguish people [18, 20]. They are collectable and quantifiable by amplitude or energy changes and hence the brain's responses to stimuli can be calibrated and measured [20]. EEG signal acquisition is applicable to most people since different forms of stimuli can trigger response signals and this accommodates for different impairments. Stimuli forms include visual, somatosensory and motor imagery [21].

Examples of media used to present visual stimulation include the Snodgrass and Vanderwart picture set which induces highly synchronized neural activity in the gamma band [22]. The Snodgrass and Vanderwart picture set is a standard set of 260 pictures drawn in black lines based on a set of rules that provide consistency in pictorial representations [20]. Lists of acronyms have also been used as stimuli for Visual Evoked Potentials [21].

EEG has been utilized for brain-computer interfaces (BCI) in medical and non-medical settings. Several applications have been derived including: automated diagnosis of epileptic EEG using entropies [24]; automated drowsiness detection using wavelet packet analysis [25]; EEG-based mild depression detection using feature selection methods and classifiers [26]; neuro-signal based lie detection [27]; authentication [20] and continuous authentication.

Several different methods have been applied for analysis of the data. Many but not all of these methods involved are machine learning based. In authentication applications, the analysis relies on a data training phase before the trained model can be used for authentication.

Model training methodology does not lend itself to flexible applicability in a forensic data collection setup. As Al Solami et al. [28] discuss, there are various limitations of these training model based schemes that makes them impractical including: biometric data is not always available in advance of events; the need for too many training samples can be impractical; behavior biometric can change between the training and testing phase; behavior biometrics can change from one context to another.

2.9 Change Point Detection in EEG Data

Al Solami et al. [28] propose a generic model of application of a change-point detection in the case of continuous authentication systems, to remove the need for prior data training and potentially increase speed. This technique has been used in detecting change points in various multivariate time series. Yu et al. [29] applied this method for detecting changes in statistical dependence within the time series, modelled using Gaussian copula graphical models. The data between the changepoints is regarded as piecewise stationary. Among various applications, the authors analyzed EEG using change point detection for the medical application of predicting epileptic seizures. During the recording of the data, the patients had experienced events that were judged to be clinical seizures by experts. Using a change point detection method two change points are observed at two seconds before the start and the end of the seizure, which is in line with the clinical specialists initial expectations.

Change point detection has also been used in conjunction with a smart home activity recognition sensor data for detecting activity transitions, segmenting the activities into separate actions and correctly identifying each action. The intended applications include timing notifications and interventions [30]. Their work involves a data training phase so as to provide activity labels needed in their model.

The non-model training property of change point detection methodologies makes the data defensible as a forensic artifact as it reduces biased manipulation and chances of distortion. The data can be used to map the onset of irregular and perhaps critical cognitive events on the part of the user, which may also signal the change of signal source.

There are several change detection algorithms with various strengths and weaknesses. The method particularly amenable to real time processing of EEG data is the cumulative sum (CUSUM) algorithm. Below is the general form of a change detection algorithm:

```
initialization
    if necessary
end
while the algorithm is not stopped do
   measure the current sample x[k]
   decide between H0 (no change) and H1 (one change)
   if H1 decided then
      store the detection time nd ← k
      estimate the change time nc
      stop or reset the algorithm
   end
end
```

Algorithm Source: Granjon [31]

The algorithm has two key components namely: **detection**: a decision between change and no change at each step; and **estimation**: of when the change occurred. The details of setup of both components are crucial from a forensic perspective, in order to reliably triangulate the onset of interesting events in or around a system.

3 Proposed Methodology

Several parts are considered in modelling the framework for EEG- based forensic evidence

I. Some forensic features of EEG and their contextual applicability as forensic artifacts
II. Forensic readiness plan for building EEG signal evidence
III. Process flow for acquisition, analysis and storage of EEG forensic data
IV. The change point detection algorithm
V. Data packaging and reduction - to reduce data management overhead
VI. Eeg evidence validation schema
VII. Other issues
    A. Anticipating Anti-forensics
    B. Privacy and Ethics Argument

I. **Some Features of EEG and Their Contextual Applicability as Forensic Artifacts**

A. **Uniqueness to Individual:** EEG Signals have unique features that can be used to distinguish between individuals. This property can be applicable if the forensic investigation is concerned with verifying that an intruder was logged into a system.

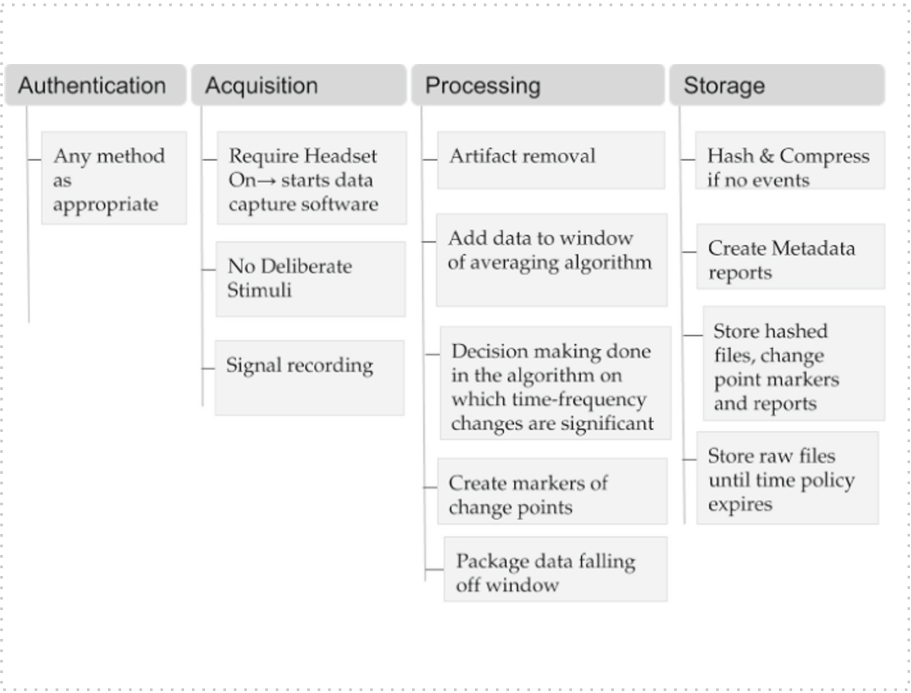
B. **Can show responses to stimuli:** The changes caused by exposure to stimuli are known as evoked potentials. These can be applicable if an investigation is concerned with verifying recognition or recall of some stimuli being shown to the subject.
Response to stimuli can also be applicable if the investigation is concerned with finding out when a unusual activity may have began around the vicinity of the person and device under investigation.

C. **EEG can show cognitive deviations:** There are five primary EEG signal bands classified by frequency. Other than that, EEG has been used to show changes in state of mind e.g. epileptic seizures, fatigue, and drowsiness as discussed earlier. This property can be applicable if an investigation is concerned with whether a person's state of cognition deviated abnormally during performance if a critical task e.g. operating critical equipment.

II. **Forensic Readiness Plan for Building EEG Signal Evidence**

Readiness Phase:	**Deployment Phase:**	**Evidence Application or Storage:**
- Identify parts of system usage where EEG data collection can be meaningful	- Collect signal	- If incident is found, provide data to forensic examiner
Select: - Headset Type - No. of channels - Data capture software	- Process signal with change detection module	- If no incident found, retain per time policy and trigger disposal procedure
	- Package signal - Build metadata, alerts etc.. - Update reports	Disposal - Analyze data - Summarize - Authorized disposal
	- Hash, compress and store signal as per time policy	

III. **Process Flow Diagram for Acquisition, Analysis and Storage of EEG Forensic Artifacts**



IV. **Change Point Detection**

There is an initial period when no averaging is done until the minimum window size is reached. The algorithm is applied with an appropriate window size to the EEG data. The EEG data collected in the sample can be decomposed and analyzed using Independent Components Analysis (ICA). A common problem in neuroimaging research results from the collection of large amounts of data which, based upon the Central Limit Theorem, become normally distributed. However, the brain is comprised of discrete patches of cortex that are very active at some points in time and relatively inactive at others (i.e., activity is not normally distributed across the scalp) [32]. ICA overcomes this problem by taking this Gaussian data and rotating it until it becomes non-Gaussian, thereby isolating independent components contributing to the activation.

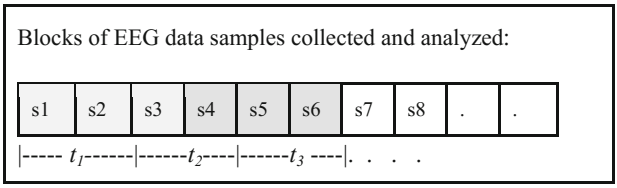
Initially, an EEGLab ICA performs a Principal Components Analysis (PCA). At each electrode site the program assesses which of the other electrode sites account for the most variance in the signal. Taking these weighted values it then relaxes the orthogonality constraint of PCA to isolate individual components of activation [32]. Each ICA component then represents a pattern of activation over the entire brain, not solely the activity present at a specific electrode. The number of independent components (ICs) depends on the number of electrodes in the dataset, as the algorithm is working in an N-dimensional space (where N is the number of electrodes). Therefore an n-channel EEG system would produce an ICA equation similar to:

$$IC_1 = w_1e_1 + w_2e_2 + \cdots w_ne_n$$

Where IC is the "Independent Component", w is the weight assigned to the electrode, and e is the electrode. The change detection algorithm that will be used for pattern detection will take in one IC as an input at each point.

V. Data Reduction and Packaging

One of digital forensic problems is the overhead of handling unwieldy volumes of data [8]. Further, processing data when it is already in duplicates, scattered and tampered with is more likely to result in invalid evidence. Data packaging and reduction is aimed at organizing data early on within the framework of a forensic ready system. Putting data into organized formats can support fast and quality analyses later if incidents happen. In this model, organization of data consists of incremental categorization, analysis, decisions, metadata, reports, hashing, compression and finally storage.



Using a time variable package blocks of data that have fallen off the left side of the change detection analysis window. After every t seconds unless event, if event, process event details first then package data. Packaging involves hashing and compression followed by labelling and storage.

VI. Evidence Validation Schema

Validity has been defined as: "the extent to which a concept, conclusion or measurement is well-founded and corresponds accurately to the real world…. validity of a measurement tool is considered to be the degree to which the tool measures what it claims to measure; in this case, the validity is an equivalent to accuracy." [33].

Boddington et al. [15] discuss that validation of digital evidence requires verifying the path of the evidence since its creation i.e. the digital environment in which it was created, processed and transferred, including the evidence file itself plus the software and hardware used in its handling. As they further discuss, If validity of evidence cannot be established then its weight is diminished or even negated.

This representation allows forensic examiner to list the relevant validity properties to check, and later add what the defending team may bring up.

	Assertion	Verification [+1]	Negation [−1]	Assertion weight
Start				
A_1				

(*continued*)

(*continued*)

	Assertion	Verification [+1]	Negation [−1]	Assertion weight
A_2				
.				
.				
A_m				
End				Total weight

Schema derived from: Boddington et al. [15]

4 Planned Study: Applicability of EEG Data for Confirming Events

In this study we plan to test the usability of EEG for triangulating the time that an event may have occurred on or around a computing system. The signal acquisition begins with general activities for the participant to use the device. At irregular but predefined intervals, we introduce a predetermined and timed cyber event. Example events include: constructing a cyber event on the participant's path by including a privilege escalation opportunity as follows: the participants will be asked to log into the test application having created an account. When they click the login link, in the form that comes up they will find the name "admin" pre-filled with a masked out password. It will look like an accidental flaw. Ideally they should erase and input their own credentials which will take them to their own account normally. However, they would be in a position to simply click enter on the admin credentials and attempt to go into admin space. The signal continues to be collected during the event intervals. We will investigate whether the signal once acquired and tested by the algorithm will be able to reveal that the events introduced occurred at given points.

5 Future Work

In this paper we have focused on turning EEG artifacts into forensic evidence. However, other physiological measurements can be similarly applicable. Some work would need to be done to determine which how the various physiological measurements can be harnessed into forensic evidence and how such models could be tested. Another questions that could be answered by further work is how to deal with anti-forensics activities such as rogue physiological data insertions and deletions as well as the creation of deliberate physiological noise during system usage where physiological data is collected.

6 Discussion and Conclusion

Many problems in cybersecurity involve individuals. Since cognition often occurs in the automatic System 1 realm, where they act in automatic mode and are unaware of specific interactions with the system. The human's system 1 or automatic behavior dimension has been largely neglected and it presents an opportunity to be applied to forensic-readiness in digital systems. Physiological responses to events can be captured and analyzed to help detect events, and when events occur, previously processed and packaged data can be readily available to facilitate the forensic investigation process. This application is especially relevant for critical systems which may include government sensitive data systems or SCADA systems which are at high risk from both internal and external threats.

References

1. Cybercrime: Legal Guidance: Crown Prosecution Service. Cps.gov.uk (2017). http://www.cps.gov.uk/legal/a_to_c/cybercrime/#a03. Accessed 28 Oct 2017
2. Holt, T., Bossler, A.: An assessment of the current state of cybercrime scholarship. Deviant Behav. **35**(1), 20–40 (2013)
3. Kahneman, D.: Thinking, Fast and Slow. Farrar, Straus and Giroux, New York (2015)
4. Stanovich, K., West, R.: Individual differences in reasoning: implications for the rationality debate? Behav. Brain Sci. **23**(5), 645–665 (2000)
5. Hausknecht, K., Gruicic, S.: Anti-computer forensics. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (2017)
6. Resendez, I., Martinez, P., Abraham, J.: An introduction to digital forensics (2017)
7. Baggili, I., Oduro, J., Anthony, K., Breitinger, F., McGee, G.: Watch what you wear: preliminary forensic analysis of smart watches. In: 2015 10th International Conference on Availability, Reliability and Security (2015)
8. Neuner, S., Mulazzani, M., Schrittwieser, S., Weippl, E.: Gradually improving the forensic process. In: 2015 10th International Conference on Availability, Reliability and Security (2015)
9. Harris, R.: Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem. Digit. Invest. **3**, 44–49 (2006)
10. Endicott-Popovsky, B.: Digital evidence and forensic readiness (2017)
11. Carrier, B., Spafford, E.: An event-based digital forensic investigation framework (2004). http://www.digital-evidence.org/papers/dfrws_event.pdf. Accessed 28 Oct 2017
12. Kazadi, J., Jazri, H.: Using digital forensic readiness model to increase the forensic readiness of a computer system. In: 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (2015)
13. Palmer, G.: Forensic analysis in a digital world. Int. J. Digit. Evid. **1**(1), 1–6 (2002)
14. Cohen, F.: Challenges to Digital Forensic Evidence, 129 p. Fred Cohen & Associates, Livermore (2008). ISBN 1-878109-41-3
15. Boddington, R., Hobbs,V., Mann, G.: Validating digital evidence for legal argument. In: Australian Digital Forensics Conference (2017)

16. Mondal, S., Bours, P.: Continuous authentication and identification for mobile devices: combining security and forensics. In: 2015 IEEE International Workshop on Information Forensics and Security (WIFS) (2015)
17. Nunez, P., Katznelson, R.: Electric Fields of the Brain. Oxford University Press, New York (1981)
18. Başar, E.: Brain Function and Oscillations. Springer, Heidelberg (1998). https://doi.org/10.1007/978-3-642-72192-2
19. Regan, D.: Human Brain Electrophysiology, pp. 1–147. Elsevier, New York (1989)
20. Zuquete, A., Quintela, B., Cunha, J.: Biometric authentication using electroencephalograms: a practical study using visual evoked potentials. Electrónica e Telecomunicações **5**(2), 185–194 (2010)
21. Palaniappan, R.: Electroencephalogram-based Brain–Computer Interface: an introduction. In: Miranda, E.R., Castet, J. (eds.) Guide to Brain-Computer Music Interfacing, pp. 29–41. Springer, London (2014). https://doi.org/10.1007/978-1-4471-6584-2_2
22. Snodgrass, J., Vanderwart, M.: A standardized set of 260 pictures: norms for name agreement, image agreement, familiarity, and visual complexity. J. Exp. Psychol. Hum. Learn. Memory **6**(2), 174–215 (1980)
23. Gui, Q., Jin, Z., Xu, W.: Exploring EEG-based biometrics for user identification and authentication. In: 2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB) (2014)
24. Acharya, U., Molinari, F., Sree, S., Chattopadhyay, S., Ng, K., Suri, J.: Automated diagnosis of epileptic EEG using entropies. Biomed. Signal Process. Control **7**(4), 401–408 (2012)
25. da Silveira, T., Kozakevicius, A., Rodrigues, C.: Automated drowsiness detection through wavelet packet analysis of a single EEG channel. Expert Syst. Appl. **55**, 559–565 (2016)
26. Li, X., Hu, B., Sun, S., Cai, H.: EEG-based mild depressive detection using feature selection methods and classifiers. Comput. Methods Programs Biomed. **136**, 151–161 (2016)
27. Cakmak, R., Zeki, A.: Neuro signal based lie detection. In: 2015 IEEE International Symposium on Robotics and Intelligent Sensors (IRIS) (2015)
28. Al Solami, E., Boyd, C., Clark, A., Islam, A.: Continuous biometric authentication: can it be more practical? In: 2010 IEEE 12th International Conference on High Performance Computing and Communications (HPCC) (2010)
29. Yu, H., Li, C., Dauwels, J.: Network inference and change point detection for piecewise-stationary time series. In: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2014)
30. Aminikhanghahi, S., Cook, D.: Using change point detection to automate daily activity segmentation. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (2017)
31. Granjon, P.: The CUSUM algorithm a small review (2012). http://chamilo2.grenet.fr/inp/courses/ENSE3A35EMIAAZ0/document/change_detection.pdf. Accessed 28 Oct 2017
32. Onton, J., Westerfield, M., Townsend, J., Makeig, S.: Imaging human EEG dynamics using independent component analysis. Neurosci. Biobehav. Rev. **30**(6), 808–822 (2006)
33. Validity (statistics): En.wikipedia.org (2017). https://en.wikipedia.org/wiki/Validity_(statistics). Accessed 28 Oct 2017