IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 8, August 2019

Present Concerns and Future Prospects of Digital Forensics

Shubham Kumar[1]

Assistant Professor, Galgotias University, Greater Noida, U.P[1]

Abstract: Given the consistently expanding predominance of innovation in present day life, there is a comparing improve in the probability of advanced gadgets being relevant to a criminal examination or common suit. As an immediate outcome, the quantity of examinations requiring computerized scientific ability is bringing about gigantic advanced proof excesses being experienced by law requirement organizations all through the world. It tends to be foreseen that the quantity of cases requiring computerized criminological examination will incredibly increment later on. All things considered, each case will require the examination of an expanding number of gadgets including PCs, cell phones, tablets, cloud-based administrations, Internet of Things gadgets, wearables, and so forth. The assortment of new computerized proof sources presents new and testing issues for the advanced agent from an ID, procurement, stockpiling and investigation point of view. This paper investigates the ebb and flow provokes adding to the excess in computerized legal sciences from a specialized stance and diagrams various future research points that could incredibly add to an increasingly productive advanced measurable procedure.

Keywords: Digital Evidence Backlog, Digital Forensic Challenges, Future Research Topics

I.INTRODUCTION

The mid 21st century has seen an emotional increment in new and regularly developing innovations accessible to customers and industry the same. Generally, the customer level client base is currently progressively proficient and learned about what technologies they utilize in their everyday lives. The quantity of situations where computerized proof is relevant to an examination is consistently expanding and it is imagined that the current accumulation for law authorization will swell in the coming a very long time as the pervasiveness of advanced gadgets increments. It is consequently that it is critical to assess the present situation in the field of computerized criminology. Cloud based administrations, Internet-of-Things gadgets, against measurable strategies, distributed and high limit stockpiling, and the sheer volume and heterogeneity of appropriate gadgets present new and testing issues for the air conditioner quisition, stockpiling and examination of this advanced evidence.

Because of the sheer volume of information to be gained, put away, examined and provided details regarding, joined with the degree of aptitude important to guarantee the court suitability of the resultant proof, it was inescapable that a huge accumulation in cases anticipating investigation would happen [Hitchcock et al., 2016]. Three specific perspectives have added to this overabundance [Quick and Choo, 2014]:

1. An increment in the quantity of gadgets that are seized for examination per case.
2. The number of cases whereby advanced evidence is considered relevant is consistently expanding.
3. The volume of possibly proof rich information put away on every thing seized is additionally expanding.

This overabundance is significantly affecting the perfect legitimate procedure. As per a re-port by the Garda Síochána Inspectorate [2015] (Irish National Police), deferrals of as long as four years in directing advanced scientific examinations on held onto gadgets have "genuinely affected on the practicality of criminal examinations" as of late. Sometimes, these postponements have brought about arraignments being rejected in courts. This issue with respect to the computerized proof overabundance is hide their aggravated because of the cross-outskirt, intra-organization collaboration required by numerous criminological examinations. On the off chance that a given nation has an especially low advanced insightful limit, it can have a critical thump on impact in an international setting [James and Jang, 2014].

In this paper, we audit pertinent late re-search writing to clarify the improvements and flow difficulties in the field. While much progress has been made in the advanced measurable procedure as of late, little work has gained appreciable ground in handling the proof build-up practically speaking. While proof is lying un-dissected in a proof store, examinations are regularly left trusting that new leads will be discovered, which has genuine ramifications for pursuing these new strings of examination sometime in the future. Various handy infrastructural improvements to the current criminological procedure are talked about including robotization of gadget acquisition and investigation, Forensics-as-

DOI 10.17148/IJARCCE.2019.8815

a-Service (FaaS), equipment encouraged heterogeneous proof expert ceasing, remote proof procurement, and traverse the Internet. These infrastructural enhancements will empower various both as good as ever legal ace cesses. These may incorporate information perception, multi-gadget proof and timetable goals, information de-duplication for capacity and securing purposes, parallel or conveyed examinations and procedure improvement of existing methods. The previously mentioned enhancements ought to com-bine to help law implementation and private digi-tal agents to significantly facilitate the current criminological procedure. It is imagined that the future research territories introduced as a component of this paper will impact further inquire about in the field.

Current Challenges

Raghavan [2013] sketched out five noteworthy test areas for advanced legal sciences, assembled from a review of research in the zone:

1. The intricacy issue, emerging from information being obtained at the most reduced (for example double) group with expanding volume and hetero-geneity, which calls for modern information decrease strategies before investigation.
2. The decent variety issue, coming about normally from consistently expanding volumes of information, yet additionally from an absence of standard methods to look at and examine the expanding numbers and sorts of sources, which bring a plurality of working frameworks, record groups, and so forth. The absence of institutionalization of computerized evidence capacity and the organizing of associated metadata likewise pointlessly adds to the multifaceted nature of sharing advanced proof among national and universal law enforcement offices [Scanlon and Kechadi, 2014].
3. The consistency and connection issue resulting from the way that current apparatuses are intended to discover parts of proof, however not to generally aid examinations.
4. The volume issue, coming about because of in-wrinkled capacity limits and the quantity of gadgets that store data, and an absence of adequate mechanization for investigation.
5. The bound together time lining issue, where multiple sources present diverse time zone references, timestamp understandings, clock slant/float issues, and the linguistic structure viewpoints involved in creating a brought together course of events.

Various different analysts have distinguished increasingly explicit difficulties, which can by and large be ordered by Raghavan's above classification. Examples incorporate Garfinkel [2010], Wazid et al. [2013], and Karie and Venter [2015]. It is broadly concurred that the volume of information that is conceivably applicable to examinations is developing quickly. The measure of information per case at the FBI's 15 provincial PC criminological research facilities has developed 6.65 occasions between 2003-2011, from 84GB to 559GB [Roussev et al., 2013]. One reason for this is the development away limits that has happened as of late. Moreover, the expanding expansion of versatile and (IoT) de-indecencies adds to the quantity of gadgets that require assessment in a given examination. Past the greatness of the information, the utilization of cloud administrations implies that it may not be clear what information exists and where it is really found.

As cutting edge versatile and wearable technologies have kept on winding up progressively pervasive among the all inclusive community, they additionally now assume an increasingly common job in advanced scientific investigations. Over the previous decade the capabilities of these shrewd gadgets have arrived at a point where they can work at a level close to that of the normal family unit PC and are at present just restricted by preparing force and capacity limit. This adds to the jumper sity issue, where a more prominent assortment of gadgets become contender for advanced measurable investigation (for example Baggili et al. [2015] has covered legal sciences on shrewd watches). Versatile and IoT de-indecencies utilize an assortment of working frameworks, record arrangements and correspondence norms, all of which add to the intricacy of computerized investigations. Moreover, inserted capacity may not be effectively removable from gadgets, dissimilar to for traditional work area and server PCs, and sometimes a gadgets will need tireless capacity completely, requiring costly RAM criminology. Researching various gadgets likewise adds to the consistency and connection issue, where proof assembled from unmistakable sources must be corresponded for transient and sensible consistency. This is frequently performed physically: a significant channel on agents' assets. The requirements for RAM legal sciences likewise moves toward becoming pertinent in instances of against criminology, where an advanced criminal takes measures to keep away from proof being gained, including the production of malware that lives in RAM alone. The expanding sophistication of computerized culprits' exercises is likewise a significant test.

Different issues incorporate constraints on transmission capacity for moving information for examination, the unpredictability of proof, the way that advanced media has a restricted life expectancy that may potentially result in evidence being lost, and the expanding pervasiveness of encryption in present day interchanges and information stockpiling. The accompanying areas focus on a number of significant rising patterns in present day computing that add to the issues laid out above.

DOI 10.17148/IJARCCE.2019.8815

1. Internet-of-Things

The Internet-of-Things (IoT) alludes to a dream of ordinary things that are associated with a system and send information to each other. Juniper Research [2015] gauge that there are as of now 13.4bn IoT gadgets in presence 2015, and they anticipate that this figure should arrive at 38.5bn by 2020. These IoT de-indecencies are regularly conveyed in two wide regions: in the shopper area (shrewd home, associated vehicles, advanced medicinal services) and in the modern space (retail, associated structures, agribusiness). Some IoT gadgets are ordinary things that have Internet availability included (for example refrigerators, TVs), while others are more up to date detecting or incitation gadgets that have been created in view of the IoT explicitly.

The IoT can possibly turn into a rich wellspring of proof from the physical world, and in that capacity it represents its very own remarkable arrangement of difficulties for advanced scientific examiners [Hegarty et al., 2014]. Contrasted with conventional computerized crime scene investigation, there is less conviction in where information started from, and where it is put away. Information tirelessness might be an issue. IoT gadgets themselves typically have restricted memory (and may have no tireless information stockpiling). In this way any information that is put away for longer periods might be put away in some in-arrange center, or sent to the cloud for progressively tireless capacity. This in this way implies the moves identified with cloud crime scene investigation (as examined beneath in Section 2.2) will probably apply in the IoT area too.

Effectively, a few endeavors have started to break down IoT gadgets for crime scene investigation purposes (for example Sutherland et al. [2014] on brilliant TVs), anyway this work is in its beginning times at present. The heterogeneous nature of IoT gadgets, incorporating differences in working frameworks, file systems and correspondence models, adds essentially to the multifaceted nature, decent variety and connection problems for measurable agents.

Ukil et al. [2011] plot some security concerns of IoT specialists, which feed straightforwardly into the wants of measurable agents, incorporating issues, for example, accessibility, legitimateity and non-revocation, which are significant for lawfully solid utilization of the information. These are promotion dressed utilizing encryption innovations, which are anything but difficult to fuse into computationally powerful gadgets that are associated with mains energy. Anyway it turns out to be to a greater degree a test for littler, battery-worked, computationally-compelled gadgets, where such contemplations might be yielded. This has unavoidable consequences for the convenience of the information in a legitimate setting.

2. Emerging Cloud Computing or Cloud Forensic Challenges

Use of cloud administrations, for example, Amazon Cloud Drive, Office 365, Google Drive and Dropbox are presently typical among most of Internet clients. From a computerized legal sciences perspective, these administrations present various extraordinary difficulties, as has been accounted for in the 2014 National Institute of Standards and Technology's draft report [NIST, 2014]. Commonly, information in the cloud is dispersed over various distinct hubs dissimilar to increasingly conventional measurable scenarios where information is put away on a solitary machine. Because of the appropriated idea of cloud administrations, information can possibly live in numerous lawful juris expressions, prompting examiners depending on nearby laws and guidelines with respect to the gathering of proof [Simou et al., 2014, Ruan et al., 2013]. This can possibly expand the time, cost and trouble related with a legal examination. From a specialized angle, the way that a wrong doing gle document can be part into various information hinders that are then put away on various remote hubs includes another layer of multifaceted nature along these lines making customary computerized scientific instruments excess [Chen et al., 2015, Almulla et al., 2013].

Moreover, the Cloud Service Providers (CSP) and their client base must be mulled over. Examiners are dependent on the eagerness of CSPs to take into consideration the obtaining and proliferation of data. The absence of standardization among the shifting CSPs, varying degrees of information security and their Service Level Agreements are deterrents to both cloud forensic scientists and specialists [Almulla et al., 2013]. The multi-tenure of many cloud systems presents three huge difficulties to digital legal investigations. In most of cases the protection and secrecy of authentic clients must be considered by investigators because of the mutual foundations that sup-port cloud frameworks [Morioka and Sharbaf, 2015]. The circulated idea of cloud frameworks alongside multi-occupancy can require the obtaining of tremendous volumes of information prompting a significant number of the difficulties sketched out beneath. At last, the utilization of IP namelessness and the simple to-utilize highlights of many cloud frameworks, for example, requiring insignificant information when pursuing an administration, can prompt circumstances where recognizing a criminal is close to unthinkable [Chen et al., 2012, Ruan et al., 2013]. Cloud legal sciences additionally faces various challenges related with customary advanced forensic investigations. Encryption and other enemy of measurable methods are regularly utilized in cloud-based crimes. The constrained time for which forensically-significant information is accessible is likewise an issue with cloud-based frameworks. Because of the way that said frameworks are persistently running information, can be overwritten whenever. Time of acquisition has likewise demonstrated a difficult errand in

DOI 10.17148/IJARCCE.2019.8815

regard to cloud legal sciences. Thethi and Keane [2012] demonstrated that ordinarily utilized scientific apparatuses, for example, the Linux dd direction and Amazon's AWS Snapshot set aside a lot of effort to procure 30Gb of information from a cloud administration.

While advances proceed concerning the instruments and systems utilized in cloud legal sciences, the previously mentioned provokes keep on blocking investigations. Henry et al. [2013] created results demonstrating that examinations on cloud-based frameworks make up just a small amount of all computerized legal examinations. Numerous examinations are slowed down past the purpose of a culprit's possessed gadgets and once in a while stretch out into the cloud-based administrations they use. Results, for example, these structure a solid contention for proceeded with research in this field.

II. FUTURE RESEARCH

1. Distributed Processing

Conveyed Digital Forensics has been talked about for quite a while [Roussev and Richard III, 2004, Shanmugasundaram et al., 2003, Garfinkel et al., 2009, Beebe, 2009]. Anyway there is more extension for it to be incorporated. Roussev et al. [2013] refer to two fundamental reasons that the handling velocity of current age computerized legal instruments is in-sufficient for the normal case: First, clients have neglected to plan unequivocal execution requirements and second, engineers have neglected to put execution as a top-level worry in accordance with dependability and accuracy. They proposed and approved another way to deal with objective securing that empowers document driven handling without disrupting ideal information throughput from the crude gadget. Their assessment of center legal star cessing capacities as for preparing rates demonstrates inborn constraints in both work area and server situations. Their outcomes propose that with current programming, staying aware of a ware SATA HDD at 120 MB/s requires somewhere in the range of 120 and 200 centers.

2. HPC and Parallel Processing

In spite of the bottleneck of numerous advanced legal tasks being circle perused speed, there are steps in the process that are not constrained by the physical read speed of the capacity gadget. For example the examination stage can expend a lot of time by PCs and people. High performance figuring (HPC) favorable circumstances ought to be utilized any place conceivable to decrease computation time, and with an end goal to lessen the time required by people. Customary HPC procedures ordinarily abuse some degree of parallelism, and to date have been underexploited by the digital measurable network. There are numerous applications where HPC systems and equipment could be utilized, for example on facilitating each piece of the computerized scientific procedure after the acquisition stage, i.e., preprocessing, capacity, investigation and revealing.

3. GPU-Powered Multi-threading

GPUs exceed expectations at "single guidance, various information" (SIMD) calculations with huge quantities of broadly useful stream processors that can execute enormously strung calculations for a number of uses and remain to do as such for some computerized crime scene investigation prerequisites in principle.

Marziale et al. [2007], noticed that GPUs have generally been both hard to program and focused at quite certain issues. More recently, multicore CPUs combined with GPU air conditioning celerators have been generally utilized in high performance processing because of better control effectiveness and execution/value proportion [Zhong et al., 2012]. Furthermore, there is currently a large number of integrand GPUs that are on a similar silicon kick the bucket as the CPU, bringing both simpler programming models and more prominent proficiency.

With new heterogeneous designs and programming models, for example, these, ground-breaking and proficient PC frameworks can be found in work-stations with straightforward access to CPU virtual locations and extremely low overhead for calculation offloading, and Power et al. [2015] have demonstrated such structures to be worthwhile in analytic handling. These appear to be very appropriate for some computerized crime scene investigation applications, especially as advancements, for example, SSDs lessen the I/O bottleneck.

In any case, the utilization of GPUs in advanced forensics is to a great extent missing from the writing and there are not many standard computerized legal devices that use GPU quickening. Marziale et al. [2007] measured the viability of offloading handling commonplace to computerized legal sciences devices, (for example, document carving) to GPUs and found noteworthy execution additions contrasted with straightforward stringing strategies on multicore CPUs. In spite of the fact that the programming of the GPUs was progressively unpredictable, the creators found that the exertion merited the exhibition gains. Collange et al. [2009] looked into the feasibility of utilizing GPUs to quicken the detection of divisions from booty records utilizing part level hashes.

Their application had the option to investigate a few plate drives at the same time and non-concurrently from one another. What's more, plates from various PCs can be investigated freely by the application. This methodology demonstrated that the utilization of GPUs is suitable.

In any case, Zha and Sahni [2011] utilized multi-design search calculations to decrease the time required for document cutting with Scalpel, demonstrating that the constraining component for execution is plate perused time. The writers state there is no advantage to utilizing GPUs, at any rate until systems to peruse the circle quicker are found. Be that as it may, this end accept just one circle, and the traditional computerized measurable model. In the new time of cloud crime scene investigation, SSDs, and other innovative developments, this I/O bottleneck will be significantly less prohibitive.

Iacob et al. [2015] have utilized GPUs in data recovery situations where reaction time is of significance, likewise to DF. They evil spirit strate noteworthy accelerate of two Bloom channel operation erations, which are utilized in estimated coordinating scientific applications [Breitinger and Roussev, 2014].

GPUs, in the same way as other new innovations, present new contemplations for computerized legal sciences. Breß et al. [2013] looked into the utilization of GPUs to star cess secret/delicate data and found that information in GPU RAM is retrievable by un-authorized clients by making a dump of gadget memory. Anyway this doesn't hinder the utilization of GPUs for handling secret data when the framework itself is just available to authorized clients.

4. DFaaS

Advanced Forensics as a Service (DFaaS) is a cutting edge augmentation of the conventional computerized measurable procedure. Since 2010, the Netherlands Forensic Institute (NFI) have actualized a DFaaS arrangement so as to battle the volume of multiplied cases [van Baar et al., 2014]. This DFaaS arrangement deals with a significant part of the capacity, computerization, examiner enquiry in the cases it man-ages. van Baar et al. [2014] depict the promotion vantages of the present framework including effective asset the board, empowering investigators to legitimately question the information, improving the pivot time between shaping a speculation in an investigation its affirmation dependent on the proof, and encouraging simpler joint effort between criminologists taking a shot at a similar case through comment and shared learning.

While the previously mentioned DFaaS framework is a huge positive development, numerous improvements to the present model could enormously speed up and enhance the present procedure. This incorporates improving the usefulness profit ready to the case investigators, improving its present ordering capacities and on-the-fly recognizable proof of implicating proof during the procurement procedure [van Baar et al., 2014].

Seeing as the DFaaS model is a cloud-based, remote access model, two huge disadvantages to the model are potential dormancy in using the online stage and being dependant on the transfer data transmission accessible during the physical capacity procurement period of the examination. A de-duplicated proof stockpiling framework, for example, that portrayed by Watkins et al. [2009], would facilitate the quicker obtaining with every interesting record over various examinations just waiting be put away, filed, dissected and clarified once on the framework. Disposing of non-relevant, generous records during the procurement period of the examination would incredibly diminish the acquisition time (e.g., working framework, application, recently obtained non-implicating documents, and so forth.). This could significantly speed up relevant information being accessible to the investigators taking a shot at the case as right on time as conceivable in the examination. All together for any proof to be court allowable, a forensically solid whole plate picture would should be re-constructible from the de-duplicated information store, enhancing the framework proposed by Watkins et al. [2009]. Utilizing such a framework would likewise encourage a cloud-to-cloud based stor-age occasion observing of virtual frameworks as only the progressions of the virtual stockpiling would should be put away between every procurement.

5. Field-programmable Gate Arrays

FPGAs are coordinated circuits that can be con-figured after assembling. FPGAs can execute any capacity that application-explicit integrated circuits can, and offer a few points of interest over conventional CPUs. FPGAs can misuse inborn algorithmic parallelism (counting low-level parallelism), and can regularly accomplish brings about less rationale activities contrasted with conventional broadly useful CPUs, bringing about quicker genius cessing times. FPGAs have as of late discovered application in zones, for example, advanced sign procedure ing, imaging and video applications, and cryptography. Regardless of showing alluring characteristics for advanced crime scene investigation analysts, they still can't seem to be abused for non-I/O-bound features of computerized criminology. Besides, as SSDs and different advances facilitate the I/O bottleneck, FPGAs remain to be all the more comprehensively material in computerized legal sciences.

6. Applying Complementary Cutting Edge Research to Forensics

Current examination practice includes the investigation of information on independent workstations. All things considered, the advancement of the procedures that can be for all intents and purposes utilized are constrained. Much research has been directed in an assortment of territories that has hypothetical importance to computerized crime scene investigation, however has been unreasonable to apply to date. A development towards DFaaS and elite processing, as examined above, offers points of interest past just speeding up the strategies presently utilized in crime scene investigation examinations, which stay dependent on manual information. It likewise guarantees a circumstance where this integral research may for all intents and purposes be presented as a powerful influence for advanced scientific examinations.

One such explore region is that of Information Retrieval (IR). Customarily, IR is worried about recognizing archives inside a corpus that help to fulfill a client's "data need". Customarily, IR scientists have been looked with the exchange off between the contending objectives of exactness (recovering just significant records) and review (recovering all the pertinent reports), whereby enhancing one of these measurements commonly brings about a decrease in the other. In IR for lawful purposes, review has for quite some time been recognized similar to the more significant measurement, given that a solitary missing important report could have genuine ramifications for the indictment of a criminal case, the implementation of an agreement, and so forth. Notwithstanding, focusing on review much of the time brings about an agent being required to physically filter through a huge amount of non-pertinent records. This is rather than web search, for instance, where clients ordinarily don't require the majority of the important reports to be recovered, of which there may perhaps be millions. Rather, a web searcher wishes to abstain from sitting around idly on non-significant material.

IR for computerized criminology is regularly observed as a typical case of legitimate data recovery (for example by Beebe and Clark [2007]). Despite the fact that this is positively valid at the point a case is being worked for court, it could be contended that the degree of review required at the triage stage can be sacrificed to some degree for more noteworthy exactness, so as to permit agents settle on expedient choices about whether a given gadget ought to be examined completely. Consequently there is the potential for configurable IR frameworks to be used in criminology investigations, whose spotlight will change contingent upon the phase of the examination.

The essential preferred position of applying IR methods to computerized examinations is that once the underlying preprocessing stage has been finished, searches can be directed incredibly rapidly. Furnas et al. [1987] has demonstrated that under 20% of searchers pick similar catchphrases for subjects they are keen on. This proposes numerous questions must be rushed to accomplish full review, and furthermore recommends that standard IR procedures, for example, inquiry extension and equivalent word coordinating could likewise be applied to build review.

Nonetheless, expanding review regularly diminishes exactness by additionally recovering non-applicable documents as false positives. There are various manners by which this issue can be lightened. The utilization of the previously mentioned information de-duplication procedures would take out standard sys-tem records from thought (Beebe and Diet-rich [2007] note that "slaughter" shows up as an order in numerous framework documents). Moreover, regular representation methodologies, for example, ranking [Beebe and Liu, 2014] and grouping [Beebe et al., 2011] are probably going to help agents in their manual hunt of recovered records.

Another thought is that occasion course of events remaking is critical in a criminal examination [Chabot et al., 2014]. When developing a course of events from advanced proof, some fleeting information is promptly accessible (for example talk logs, document alteration times, email times-packs, and so on.), in spite of the fact that it ought to be recognized that even this isn't without its own difficulties. Inside the IR people group, much research has been led into the extraction of beat ral data from unstructured content [Campos et al., 2014]. This can be utilized to drastically decrease the manual burden on examiners around there.

III. CONCLUSION

In this paper various current difficulties in the field of computerized crime scene investigation are talked about. Every one of these difficulties in disconnection can hamper the disclosure of appropriate data for advanced investigators and criminologists associated with a multitude of various cases requiring computerized legal examination. Joined, the negative impact of these difficulties can be incredibly intensified. These is-sues close by constrained aptitude and colossal outstanding burdens has brought about the advanced proof overabundance expanding to the request for years for some law requirement offices around the world. The predicted swelling of case volume in the close future will serve to further aggravate the accumulation issue – especially as the volume of proof from non-conventional sources, for example, cloud-based and Internet-of-Things sources, is additionally liable to increment. As far as research bearings, rehearses al-prepared set up in numerous Computer Science sub-disciplines hold guarantee for tending to these difficulties incorporating those in circulated, parallel, GPU and FPGA handling, and information recovery. Progressively shrewd de-duplicated evidence information stockpiling and examination systems can help wipe out the copied preparing and duplicated master investigation of beforehand content. These exploration bearings can be applied to the customary computerized legal sciences procedure to help com-bat the previously mentioned accumulation through more efficient allotment of valuable advanced legal ex-energetic time through the improvement and endeavor of the procedure itself.

REFERENCES

[1]. S. Almulla, Y. Iraqi, and A. Jones. Cloud Forensics: A Research Perspective. In Innovations in Information Technology (IIT), 2013 9th International Conference on, pages 66–71, March 2013.

[2]. Ibrahim Baggili, Jeff Oduro, Kyle Anthony, Frank Breitinger, and Glenn McGee. Watch What You Wear: Preliminary Forensic Analysis of Smart Watches. In 2015 10th International Conference on Availability, Reliability and Security, pages 303–311. IEEE, Aug 2015. ISBN 978-1-4673-6590-1.

[3]. Nicole Beebe. Digital Forensic Res: The Good, Bad & the Unaddressed. In Advances in Digital Forensics V, p.no:17–36 Springer, 2009.

[4]. Nicole Beebe & Glenn Dietrich. A New Process Model for Text String Search. In Advance in Digital Forensic 3, 179–191 Springer, 2007

[5]. Nicole Lang Beebe and Jan Guynes Clark. Digital Forensic Text String Searching: Improving Information Retrieval Effectiveness by

DOI 10.17148/IJARCCE.2019.8815

Thematically Clustering Search Results. Digital Investigation, 4(S1):49–54, 2007.

[6]. Nicole Lang Beebe & Lishu Liu. Ranking Algorithm for Digital Forensic String Search Hits. Digital Investigation, 11(S2):314–322, 2014

[7]. Nicole Lang Beebe, Jan Guynes Clark, Glenn B. Dietrich, Myung S. Ko, and Daijin Ko. Post-Retrieval Search Hit Clustering to Improve Information Retrieval Effectiveness: Two Digital Forensics Case Studies. Decision Support Systems, 51(4):732–744, 2011.

[8]. Frank Breitinger and Vassil Roussev. Automated Evaluation of Approximate Matching Algorithms on Real Data. Digital Investigation, 11:S10–S17, 2014.

[9]. Sebastian Breß, Stefan Kiltz, and Martin Schäler. Forensics on GPU Coprocessing in Databases–Research Challenges, First Experiments, and Countermeasures. In BTW Workshops, pages 115–129. Citeseer, 2013.

[10]. Ricardo Campos, Gaël Dias, Alípio M Jorge, & Adam Jatowt. Survey of Temporal Information Retrieval & Related Applications. ACM Computing Surveys (CSUR), 47(2):15, 2014.

[11]. Yoan Chabot, Aurélie Bertaux, Tahar Kechadi, and Christophe Nicolle. Event Reconstruction: A State of the Art.

[12]. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance, page 15, 2014.

[13]. Guangxuan Chen, Yanhui Du, Panke Qin, and Jin Du. Suggestions to digital forensics in cloud computing era. In Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on, pages 540–544, Sept 2012.

[14]. Lei Chen, Lanchuan Xu, Xiaohui Yuan, and N. Shashidhar. Digital Forensics in Social Networks and the Cloud: Process, Approaches, Methods, Tools, and Challenges. In Computing, Networking and Communications (ICNC), 2015 International Conference on, pages 1132–1136, Feb 2015.

[15]. Sylvain Collange, Yoginder S Dandass, Marc Daumas, and David Defour. Using graphics processors for parallelizing hash-based data carving. In System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on, pages 1–10. IEEE, 2009.

[16]. George W. Furnas, Thomas K. Landauer, Louis M. Gomez, and Susan T. Dumais. The Vocabulary Problem in Human-System Communication. Communications of the ACM, 30(11):964–971, 1987.

[17]. Garda Síochána Inspectorate. Changing Policing in Ireland, November 2015.

[18]. Simson Garfinkel, Paul Farrell, Vassil Roussev, and George Dinolt. Bringing Science to Digital Forensics with Standardized Forensic Corpora. Digital Investigation, 6:S2–S11, 2009.

[19]. Simson L Garfinkel. Digital Forensics Research: The Next 10 Years. Digital Investigation, 7: S64–S73, 2010.

[20]. Robert C. Hegarty, David J. Lamb, and Andrew Attwood. Interoperability Challenges in the Internet of Things. In Paul Dowland, Steven Furnell, and Bogdan Ghita, editors, Proceedings of the Tenth International Network Conference (INC 2014), pages 163–172. Plymouth University, 2014.

[21]. Paul Henry, Jacob Williams, & Benjamin Wright. The SANS Survey of Digital Forensics and Incident Response. In Tech Rep, Jul 2013

[22]. Ben Hitchcock, Nhien-An Le-Khac, and Mark Scanlon. Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists. Digital Investigation, 13 (S1), 03 2016. Proceedings of the Third Annual DFRWS Europe.

[23]. Alexandru Iacob, Lucian Itu, Lucian Sasu, Florin Moldoveanu, and Constantin Suciu. Gpu accelerated information retrieval using bloom filters. In System Theory, Control and Computing (ICSTCC), 2015 19th International Conference on, pages 872–876. IEEE, 2015.

[24]. Joshua I James and Yunsik Jake Jang. Measuring Digital Crime Investigation Capacity to Guide International Crime Prevention Strategies. In Future Information Technology, pages 361–366. Springer, 2014.

[25]. Juniper Research. The Internet of Things: Consumer, Industrial & Public Services 2015-2020, July 2015.

[26]. Nickson M Karie and Hein S Venter. Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, 60(4):885–893,2015.

[27]. Lodovico Marziale, Golden G Richard, and Vassil Roussev. Massive Threading: Using GPUs to Increase the Performance of Digital Forensics Tools. Digital Investigation, 4: 73–81, 2007.

[28]. E. Morioka and M.S. Sharbaf. Cloud Computing: Digital Forensic Solutions. In Information Technology - New Generations (ITNG), 2015 12th International Conference on, pages 589–594, April 2015.

[29]. NIST. NIST Cloud Computing Forensic Science Challenges. 2014.

[30]. Jason Power, Yinan Li, Mark D Hill, Jignesh M Patel, & David A Wood. Toward GPUs Being Mainstream in Analytic Process 2015

[31]. Darren Quick and Kim-Kwang Raymond Choo.

[32]. Impact of Increasing Vol of Digital Forensic Data: A Survey & Future Research Challenges. Digital Investigation, 11(4): 273–294, 2014.

[33]. Sriram Raghavan. Digital Forensic Research: Current State of the Art. CSI Transactions on ICT, 1(1):91–114, 2013.

[34]. Vassil Roussev and Golden G Richard III. Breaking the Performance Wall: The Case for Distributed Digital Forensics. In Proceedings of the 2004 Digital Forensics Research Workshop (DFRWS), volume 94, 2004.

[35]. Vassil Roussev, Candice Quates, and Robert Martell. Real-time Digital Forensics and Triage. Digital Investigation, 10(2):158–167, 2013.

[36]. Keyun Ruan, Joe Carthy, Tahar Kechadi, and Ibrahim Baggili. Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability: An Overview of Survey Results. Digital Investigation, 10(1):34 – 43, 2013.

[37]. Mark Scanlon & M-Tahar Kechadi. Digital Evidence Bag Selection for P2P Network Investigation. In Proceedings of the 7th Internat Symposium on Digital Forensics and Information Security (DFIS-2013), pages 307–314. Springer, Gwangju, South Korea, 2014.

[38]. Kulesh Shanmugasundaram, Nasir Memon, Anubhav Savant, and Herve Bronnimann. ForNet: A Distributed Forensics Network. In Computer Network Security, pages 1–16. Springer, 2003.

[39]. Stavros Simou, Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. Cloud Forensics Solutions: A Review. In Lazaros Iliadis, Michael Papazoglou, and Klaus Pohl, editors, Advanced Information Systems Engineering Workshops, volume 178 of Lecture Notes in Business Information Processing, pages 299–309. Springer International Publishing, 2014. ISBN 978-3-319-07868-7.

[40]. Iain Sutherland, Huw Read, and Konstantinos Xynos. Forensic Analysis of Smart TV: A Current Issue and Call to Arms. Digital Investigation, 11(3):175–178, sep 2014.

[41]. Neha Thethi and Anthony Keane. Digital Forensics Investigations in the Cloud. In IEEE International Advance Computing Conference (IACC), Sept 2012.

[42]. Arijit Ukil, Jaydip Sen, and Sripad Koilakonda. Embedded Security for Internet of Things. In 2011 2nd National Conference on Emerging Trends and Applications in Computer Science, pages 1–6. IEEE, mar 2011. ISBN 978-1-4244-9578-8.

[43]. RB van Baar, HMA van Beek, & EJ van Eijk. Digital Forensic as a Service: A Game Changer. Digital Investigation, 11:S54–S62, 2014

[44]. Kathryn Watkins, Mike McWhorte, Jeff Long, and Bill Hill. Teleporter: An Analytically and Forensically Sound Duplicate Transfer System. Digital Investigation, 6:S43–S47, 2009.

[45]. Mohammad Wazid, Avita Katal, RH Goudar, and Smitha Rao. Hacktivism Trends, Digital Forensic Tools and Challenges: A Survey. In Information & Communication Technologies (ICT), 2013 IEEE Conference on, pages 138–144. IEEE, 2013.