



Annual ADFSL Conference on Digital Forensics, Security and Law

2017
Proceedings

May 16th, 1:30 PM

Digital Forensics Tool Selection with Multi-armed Bandit Problem


Umit Karabiyik

Sam Houston State University, umit@purdue.edu

Tugba Karabiyik

Sam Houston State University, tugba@shsu.edu

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Sciences Commons](#), [Design of Experiments and Sample Surveys Commons](#), [Forensic Science and Technology Commons](#), and the [Probability Commons](#)

Scholarly Commons Citation

Karabiyik, Umit and Karabiyik, Tugba, "Digital Forensics Tool Selection with Multi-armed Bandit Problem" (2017). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 14.
<https://commons.erau.edu/adfsl/2017/papers/14>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



DIGITAL FORENSICS TOOL SELECTION WITH MULTI-ARMED BANDIT PROBLEM

Umit Karabiyik¹ and Tugba Karabiyik²

¹Department of Computer Science

²Department of Mathematics and Statistics

Sam Houston State University

Huntsville, Texas, USA

{umit,tugba}@shsu.edu

ABSTRACT

Digital forensics investigation is a long and tedious process for an investigator in general. There are many tools that investigators must consider, both proprietary and open source. Forensics investigators must choose the best tool available on the market for their cases to make sure they do not overlook any evidence resides in suspect device within a reasonable time frame. This is however hard decision to make, since learning and testing all available tools make their job only harder. In this paper, we define the digital forensics tool selection for a specific investigative task as a multi-armed bandit problem assuming that multiple tools are available for an investigator's use. In addition, we also created set of disk images in order to create a real dataset for experiments. This dataset can be used by digital forensics researchers and tool developers for testing and validation purposes. In this paper, we also simulated multi-armed bandit algorithms to test whether using these algorithms would be more successful than using simple randomization (non-MAB method) during the tool selection process. Our results show that, bandit based strategies successfully analyzed up to 57% more disk images over 1000 simulations. Finally, we also show that our findings satisfy a high level of statistical confidence. This work will help investigators to spend more time on the analysis of evidence than learning and testing different tools to see which one performs better.

Keywords: Digital Forensics Tools, Digital Investigations, Multi-armed Bandit Problem, Decision Making

1. INTRODUCTION

Digital forensics, a branch of forensic science, deals with the investigation and recovery of digital information found in digital devices which are mostly found at crime/incident scenes or belonging to suspects. Digital

forensics is becoming increasingly needed in this early twenty-first century because of the technological advances in today's world. Most data are now being stored in digital forms such as pictures, diaries, calendars, videos, and even our DNA information.

Smart phones, tablets, computers, and wearable devices have already become a part of most people's everyday life. This inevitable change makes any device's storage a potential evidence related to a crime or an incident.

Digital evidence for a variety of crimes including child pornography, financial fraud, identity theft, cyberstalking, homicide, abduction and rape can be collected by using digital forensics techniques and tools. Digital forensics investigators use specialized and general purpose digital forensics tools in order to collect useful information or evidence that is related to a crime or incident.

Digital forensics is generally a long and tedious process for an investigator (Nelson, Phillips, & Steuart, 2015). There are many tools that an investigator must consider, both proprietary and open source. Researchers and tool developers regularly make newer tools available, particularly open source. Most of the general purpose tools have similar capabilities along with their unique properties. There are also task specific open source tools which perform similar tasks on a given device. Investigators generally decide to use certain tools based on their familiarity, technical skills, and previous experiences on those tools. In addition, they may sometimes have to use additional tools to verify their findings. This is commonly the case when their previously selected tools do not generate desired output.

Multi-armed bandit problem is a well-known problem in probability theory and machine learning (Berry & Fristedt, 1985). It is a problem of decision making when a gambler has multiple slot machines to play. Each machine looks the same but has an independent unknown probability of success and yields a reward. The gambler faces with a conflict in term of which machine to play, how long to play each machine and in what order to play the machines in order

to maximize his/her total reward (Weber et al., 1992). This conflict is called *Exploration vs Exploitation Dilemma*. Exploitation suggests the player to make the best decision based on the given current information while Exploration recommends to collect more information to play (Gittins & Whittle, 1989; White, 2013).

In this paper, we define the digital forensics tool selection for a specific task as a multi-armed bandit problem assuming that multiple tools are available for an investigator's use on each task. We specifically choose file carving task in this work. In order to test the decision quality and determine initial probability of success of each tool, we created a dataset of 100 disk images using forensic test image generator (ForGe) (Visti, 2017). We then ran widely used carving tools scalpel (Richard & Marziale, 2017) and photorec (Grenier, 2017) on these disk images by treating each tool as an individual arm used in multi-armed bandit problem. Based on the analysis results we retrieved, we compared the average reward yielded by each algorithm based on their successes and failures against to randomization method (non-MAB method) over 1000 simulations. Our results show that, an investigator would have successfully analyzed the given disk images up to 57% more, if their decisions were based on multi-armed bandit algorithms rather than random selection. We also show how multi-armed bandit algorithms behave differently based on the running time of an individual tool on each disk image and the number of evidence files retrieved from the disk images. In addition, we also supported our experimental results with a good level of statistical confidence by finding p-values using χ^2 test for independence.

To the best of our knowledge, multi-armed bandit problem has not been applied to the decision making process in digital forensics

tool selection for certain investigative tasks in the computer forensics literature. One possible reason could be the issues related to the admissibility of evidence when the decision is made by non-human entities such as software programs. However, we believe that it would not be an issue since investigators are not expected to know the details of tools or systems that they use during the examination as long as their findings are reproducible by others (Nelson et al., 2015). Therefore, the contributions of this study to the digital forensics literature is threefold; first, experimental study of multi-armed bandit problem is applied to the computer forensics domain. Second, digital forensics tool selection problem is optimized and made available for easy adaptation to automated digital forensics tools. Third, publicly available dataset of 100 disk images with hidden data is created for digital forensics researchers and tool developers' use. We also believe that the proposed model can be used by investigators in order to test their preferred tools against to set of other available tools. With this, investigators may have better idea of using certain tools in specific order and switch them when needed.

This paper is organized as follows. The following section provides related work in which multi-armed bandit problem is applied to various domains in computer science and specifically to networks forensics. Section 3 discusses existing multi-armed bandit algorithms that are implemented and used in this paper. Section 4 explains the experimental design for both the dataset creation and simulation. In Section 5 we demonstrate our results obtained from 1000 simulations. Finally, the last section concludes our study with some recommendations.

2. RELATED WORK

The multi-armed bandit problem has been widely applied to many areas from clinical trials (Berry & Fristedt, 1985; Gittins & Whittle, 1989; Press, 2009; Kuleshov & Precup, 2014; Vermorel & Mohri, 2005) to Internet search engines (Lu, Pál, & Pál, 2009, 2010)(e.g. Google) and websites (White, 2013) in order to optimize decision making process. However, multi-armed bandit problem has been rarely applied to digital forensics problems although digital forensics investigators also deal with many decision making conflicts. In this section we briefly explain the research efforts mainly targeting issues in network forensics which we find them most related work to our study.

Yu et al. studied the problem of monitoring passive secondary users in an unslotted Cognitive Radio Networks (CNRs) in (Yi, Zeng, & Xu, 2012). This work shows how a monitoring assignment policy for network sniffer tools can be designed by using multi-armed bandit problem in order to help network administrators and forensic investigators to collect interesting user data from the networks.

In (Xu, Wang, Jin, Zeng, & Liu, 2014), Xu et al. have also studied a similar secondary user data capturing problem and formulated dynamic sniffer channel assignment problem as a non-stochastic multi-armed bandit problem. The purpose of their study is to maximize the total number of the sniffed or effectively monitored secondary user traffic, and thus increase the collection of forensic data.

Similarly, Li et al. have adapted multi-armed bandit problem to the deployment problem of monitoring algorithms for adversarial spectrum usage in CRNs' channels and developed two algorithms, SpecWatch and SpecWatch+ (Li, Yang, Lin, & Tang, 2016). The proposed model is designed by taking

switching costs of the monitoring on multiple channels into account.

To the best of our knowledge none of this work is directly applied to decision making process of a digital forensics investigator, rather they provide forensic data collection in an optimal way for further analysis.

3. MULTI-ARMED BANDIT ALGORITHMS

Multi-armed bandit problem is a difficult problem in its nature as Peter Whittle points this out by saying: “Sir, the multi-armed bandit problem is not of such a nature that it can be solved” in (Gittins & Whittle, 1989). However, there are approximate solutions to this problem as discussed below. In this paper, we compare several multi-armed bandit algorithms such as ϵ -greedy algorithm (Kuleshov & Precup, 2014), ϵ -first algorithm, Softmax algorithm (Sutton & Barto, 1998) and the simplest algorithm of the Upper Confidence Bounds (UCB) family, UCB1 (Auer, Cesa-Bianchi, & Fischer, 2002) against to simple randomization on the problem of digital forensics tool selection.

First two algorithms, ϵ -greedy and ϵ -first, are known as semi-uniform strategies which are the simplest approximate solutions to the multi-armed bandit problem. These algorithms have a greedy behavior which suggest to pull the best arm (choosing the best tool in tool selection problem) based on exploitation except when a random action is taken by exploration. On the other hand, Softmax algorithm selects the best arm with a probability that is proportional to its average reward. Lastly, UCB1 algorithm is known as an approximate solution to the contextual bandit problem and makes decisions based on an expected regret (Kuleshov & Precup, 2014). Below, we briefly explain and discuss each algorithm. However, we will not dis-

cussed the proofs as it is out of the scope of this paper.

3.1 ϵ -greedy Algorithm

The ϵ -greedy algorithm is a pure random process and the decision is made randomly when strategy is switched from exploitation to exploration. The algorithm play the current best reward yielding arm with the probability $1 - \epsilon$, and selects a random arm with probability ϵ at each round $t = 1, 2, \dots$. This also can be expressed as, given initial empirical means $\mu_1(0), \dots, \mu_K(t)$ and $p_i(t)$ which represents the probability of picking arm i at time t ,

$$p_i(t+1) = \begin{cases} 1 - \epsilon + \frac{\epsilon}{k}, & i = \arg \max_{j=1, \dots, K} \mu_j(t) \\ \frac{\epsilon}{k}, & otherwise \end{cases} \quad (1)$$

In our experiments, we consider only fixed value of $\epsilon = 0.15$.

3.2 ϵ -first Algorithm

ϵ -first algorithm suggests pure exploration phase which is then followed by a pure exploitation phase. Exploration happens in the first ϵN trials which randomly selects an arm. The exploitation happens in the rest of the $(1 - \epsilon)N$ trials by selecting the best arm for the total of N trials. For instance, if $N = 1000$ meaning the number of trials and $\epsilon = 0.15$, then ϵ -first algorithm suggests selecting the best arm for the first 150 trials, and selecting an arm in rest of 850 trials at random.

Similar to the ϵ -greedy algorithm, we consider only fixed value of $\epsilon = 0.15$ in our experiments.

3.3 Softmax Algorithm

The Softmax algorithm selects an arm using Boltzman distribution which is used to describe how groups of particles behave

in physics. The higher the temperature, the more randomly behaves the particles. Hence, given same empirical means above,

$$p_i(t+1) = \frac{e^{\frac{\mu_i(t)}{\tau}}}{\sum_{j=1}^k e^{\frac{\mu_j(t)}{\tau}}}, i = 1 \dots n \quad (2)$$

τ is called a temperature parameter which controls the randomness of the decision process. In our experiments, we only use fixed value of $\tau = 0.1$ as suggested by (Kuleshov & Precup, 2014).

3.4 UCB1 Algorithm

UCB family algorithms keep track of how much it knows and what it knows about any of the arms available to them. UCB1 can make decisions to explore by our confidence in the estimated value of the arms we have selected and it does not use randomness unlike ϵ -greedy, ϵ -first and Softmax algorithms (White, 2013).

UCB1 algorithm initially assumes that each arm is played at least once, and the number of times that each arm has been played shown by $n_i(t)$. Then, UCB1 algorithm selects the arm $j(t)$ at round t as follows:

$$j(t) = \arg \max_{i=1 \dots k} \left(\mu_i + \sqrt{\frac{2 \ln(t)}{n_i}} \right) \quad (3)$$

One the most important measures on an algorithms performance is known as the *total expected regret*. It can be defined as the difference between the total expected reward from the best arm, and the total empirical means. It is also shown by (Auer et al., 2002), the expected regret of UCB1 at turn t is bounded by the following:

$$8 \sum_{i: \mu_i < \mu^*} \frac{\ln(t)}{\Delta_i} + \left(1 + \frac{\pi^2}{3}\right) \sum_{i=1}^k \Delta_i \quad (4)$$

where $\Delta_i = \mu^* - \mu_i$. The bound on the regret from above is known to be $O(\log n)$, hence UCB1 achieves the optimal regret. This also results the success on solving the multi-armed bandit problem.

4. EXPERIMENTAL SETUP

In this section, we explain how we created our test disk images, collected data, and designed simulation environment in details.

4.1 Forensic Disk Image Creation

In order to test aforementioned multi-armed bandit algorithms in our simulations, we needed to have initial probability of success of each file carving tool (Scalpel and Photorec) based on their performances in series of investigations. Therefore, we created 100 disk images using ForGe, a forensic test image generator. Each disk image contains set of files (including forensically interesting files) in allocated space and unconventional areas such as slack space, unallocated space (for deleted files), and free space.

As the first step, we setup up a “case” in which we generate disk images of 250MB in size with sector size of 512 bytes and cluster size of 8 sectors (4KB). Our case is set up to create an NTFS file system on the disk image as the type of the file system has minimal effect on the file carving process. In the next step, we created the “trivial strategy” which represents the files normally found in the file system’s allocated space. We filled the allocated space with randomly chosen files gathered from Digital Corpora (Garfinkel, Farrell, Roussev, & Dinolt, 2009) using similar methods discussed in (Karabiyik & Aggarwal, 2016).

At the final step of disk creation, we hid horse pictures (representing files containing

illegal contents) to the hidden areas on disks. We had various sizes of horse pictures as we need files less than 4K in size to be stored on the slack space. As a result, we created 100 disk images with NTFS file system and contain various file types stored on allocated, slack, unallocated, and free spaces. Reports on the details of disk image creation process and hidden files with their locations are available for interested researchers and tool developers upon request.

4.2 Tool Execution and Data Collection

After we created all disk images to test carving tools, we wrote a Python script to run Scalpel and Photorec on each disk image and recorded the processing time of each tool on each disk as well as the carved files. Both tools are configured to carve only picture files such as *jpeg*, *png*, and *gif*. Based on the collected results with respect to execution time and number of carved horse pictures, we calculated the initial probability of success value of each tool for the following three cases.

- **Time sensitive case:** In this case, the time is critically important for an investigator. Therefore, we give more weight to the faster tool when assigning reward values.
- **File sensitive case:** In this case, the total number of successfully carved illegal files is critically important. Therefore, the tool carving all the illegal files is considered successful and thus given more weight.
- **Equally sensitive case:** In this case, time and file sensitivity are considered equally important and both tools are given equal weights.

These three cases are chosen mainly because, depending on the digital forensics case, investigator may be interested in finishing the investigation faster than finding all the possible evidence especially when at least one evidence is enough, and vice versa.

In order to calculate the initial probability of success of each tool we need to assign reward values (1 for success and 0 for failure) to each tool depending on their results. In the first case, we assigned reward value to the faster tool as 1. When one tool succeeds, it is also possible for other tool to be successful. Therefore, we compared the running time of the slower tool (t_s) to faster tool (t_f), and assigned slower tool's reward value (r_s) as:

$$r_s = \begin{cases} 0, & \text{if } (t_s)^2 < t_f \\ 1, & \text{otherwise} \end{cases} \quad (5)$$

After assigning all the reward values to both tools, we calculated the initial probability of success of each tool for all three cases mentioned above (see Table 1 for initial probability of success values). Note that, we will refer the probability of success of each tool as their reward value in the rest of this paper.

Table 1: Initial reward values of Scalpel and Photorec for all three cases

Sensitivity	Scalpel	Photorec
Equal Sensitive	0.16	0.5
Time Sensitive	0.23	1
File Sensitive	0.85	0.5

As Table 1 shows, Photorec was given reward value of 1 in time sensitive case, because it outperformed Scalpel in most of the test cases with respect to execution time. In rare test cases, Scalpel outperformed Photorec, however Photorec's execution time has never been small enough to satisfy the first

condition in Equation 5. Thus, in such test cases, both tools were considered successful with respect to their execution times, hence both were given reward value of 1.

In file sensitive case, Scalpel was more successful than Photorec with respect to number of successfully carved files. The only condition that Scalpel failed was, when files were located in the slack space and fragmented. In such cases, some of the fragments were carved however we considered tools being successful if the pictures contained large portion of horse bodies. When horse bodies were not recognized, we considered tools failed. On the other hand, Photorec was failed carving the files from all locations including allocated, slack, and unallocated spaces in different test cases. We do not further discuss the reasons of failures or successes as tool testing is out of the scope of this work.

The simulation was implemented in Java programming language and source code of our program is available upon request. We performed 1000 simulations for all five tool selection strategies (the bandit algorithms and simple randomization) on given 100 disk images for both carving tools. All the results presented in this paper represent an average over these 1000 simulations. Note that, with simple randomization we mean to choose each tool at random.

Each simulation is performed as follows. A total of 100 disk images were analyzed for illegal picture search by two carving tools. The tool selection strategy (the bandit algorithms and randomization) picks a tool for each disk image with given parameters when needed. Therefore, we used $\epsilon = 0.15$ for both ϵ -greedy and ϵ -first algorithms, and temperature value $\tau = 0.1$ for Softmax algorithm. We discuss our simulation results in the following section.

Table 2: Number of disk images successfully analyzed

Sensitivity	Algorithm	Avg total reward
Equal Sensitive	ϵ -greedy	44.693
	ϵ -first	41.378
	Softmax	46.818
	UCB1	43.236
	Randomization	32.96
Time Sensitive	ϵ -greedy	92.03
	ϵ -first	86.408
	Softmax	96.507
	UCB1	93.514
	Randomization	61.619
File Sensitive	ϵ -greedy	79.598
	ϵ -first	72.148
	Softmax	74.909
	UCB1	78.299
	Randomization	67.701

5. SIMULATION RESULTS

In this section we present our results for decision making process on tool selection for data carving task by comparing available multi-armed bandit algorithms including ϵ -greedy, ϵ -first, Softmax and UCB1 against to simple randomization method. We also show how these algorithms would be beneficial if they were used during the tool selection process by presenting average number of successfully analyzed disk images. By presenting contingency tables for all algorithms, we also show how successful each tool is when they are selected by an individual strategy with high level of statistical confidence.

In Table 2, we present the average number of disk images successfully analyzed (shown in column *Avg total reward*) over 100 disk

images for 1000 simulations. According to the our results, it is clear that if bandit algorithms would be followed during the decision making process, average number of successfully analyzed disk images would increase up to 42% and 57% in equal sensitive and time sensitive cases respectively. Similarly, success increase for file sensitive case would be up to 18%.

Tables 3, 4 and 5 show the average number of successes and failures of each tool in details for every algorithm in all three sensitivity cases. Although our results show the success of multi-armed bandit algorithms against to the randomization strategy on tool selection, we still need to support this finding with a good level of statistical confidence (with a small p-value, $p < 0.05$). Hence, we calculated p-values by using χ^2 test for independence. It is important to note that, despite the weakness of the χ^2 test for independence compared to more advanced statistical approaches (Kuleshov & Precup, 2014), the p-values we found substantiate our findings for the tool selection problem.

Figures 1, 2 and 3 show the number of average disk images successfully analyzed for each disk with the average being taken over the 1000 simulations. In each figure, we compared the performance of simple randomization method with each bandit algorithm for all three cases.

6. CONCLUSION

Digital forensics investigators have multiple tools that perform the same task and they need to choose the best tool among them. However, they generally do not have plenty of time to test which tool performs better with respect to execution time and results generated. In addition, a particular tool may not perform similarly in different investigations. Therefore, digital forensics investiga-

tors commonly select the tools which they are most familiar with and switch them when the tools do not yield desired results.

The aim of this paper is to show how this decision making process can be simplified for investigators using multi-armed bandit problem in tool selection since reducing the burden on the shoulders of an investigator is always welcomed by the digital forensics community (Beebe, 2009). This work also can be adapted to automated systems when they integrate open source tools which perform similar tasks and thus tool selection could be automated too. This will help an investigator to spend more time on the analysis of evidence than learning and testing different tools to see which one performs better. In addition, we also created set of disk images in order to create a real dataset for experiments. This dataset can be also used by digital forensics researchers and tool developers for testing and validation purposes (Access link: <http://www.shsu.edu/uxk006/research.html>).

In this paper, we simulated multi-armed bandit algorithms to test whether using these algorithms during the tool selection process would be more successful than using simple randomization. Our results show that, bandit based strategies successfully analyzed up to 57% more disk images. At the end, we also supported our findings with a good level of statistical confidence.

In addition, we believe this work will open new application areas regarding adaptation of multi-armed bandit problem to various digital forensics related areas. For instance, it could be applied to industrial systems forensics and Internet of Things (IoT) forensics to use available tools with automated selection. It may also be studied further in network forensics specifically in intrusion detection systems (IDS) as there could be multiple IDSs producing multiple logs. Last but not least, the multi-armed bandit prob-

Table 3: Contingency table of bandit algorithms for carving tools for equally sensitive case

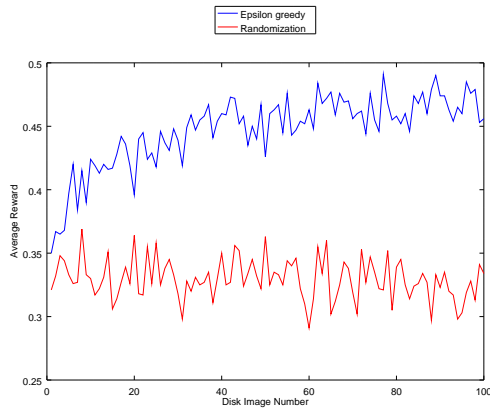
Algorithm	Contingency Table				p-value
ϵ -greedy		Success	Failure	Total	1.3×10^{-2}
	Scalpel	2.396	12.857	15.253	
	Photorec	42.297	42.45	84.747	
	Total	44.693	55.307	100	
ϵ -first		Success	Failure	Total	3×10^{-3}
	Scalpel	3.959	20.897	24.856	
	Photorec	37.419	37.725	75.144	
	Total	41.378	58.622	100	
Softmax		Success	Failure	Total	4.9×10^{-2}
	Scalpel	1.455	7.705	9.16	
	Photorec	45.363	45.477	90.84	
	Total	46.818	53.182	100	
UCB1		Success	Failure	Total	5×10^{-3}
	Scalpel	3.263	17.257	20.52	
	Photorec	39.973	39.507	79.48	
	Total	43.236	56.764	100	
Randomization		Success	Failure	Total	2.9×10^{-4}
	Scalpel	8.023	42.139	50.162	
	Photorec	24.937	24.901	49.838	
	Total	32.96	67.04	100	

Table 4: Contingency table of bandit algorithms for carving tools for time sensitive case

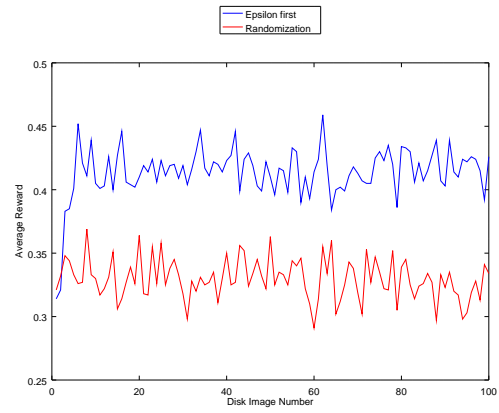
Algorithm	Contingency Table				p-value
ϵ -greedy		Success	Failure	Total	0.0
	Scalpel	2.451	7.97	10.421	
	Photorec	89.579	0	89.579	
	Total	92.03	7.97	100	
ϵ -first		Success	Failure	Total	0.0
	Scalpel	4.029	13.592	17.621	
	Photorec	82.379	0	82.379	
	Total	86.408	13.592	100	
Softmax		Success	Failure	Total	0.0
	Scalpel	1.012	3.493	4.505	
	Photorec	95.495	0	95.495	
	Total	96.507	3.493	100	
UCB1		Success	Failure	Total	0.0
	Scalpel	2.03	6.486	8.516	
	Photorec	91.484	0	91.484	
	Total	93.514	6.486	100	
Randomization		Success	Failure	Total	2.6×10^{-15}
	Scalpel	11.545	38.381	49.926	
	Photorec	50.074	0	50.074	
	Total	61.619	38.381	100	

Table 5: Contingency table of bandit algorithms for carving tools for file sensitive case

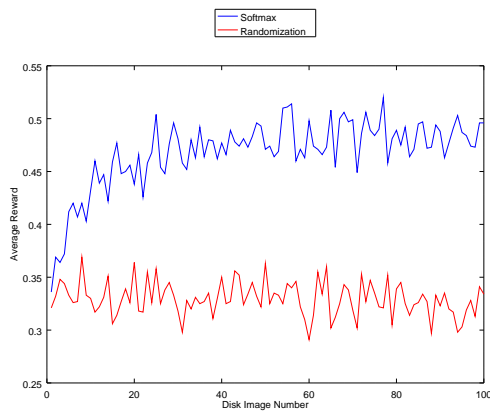
Algorithm	Contingency Table				p-value
ϵ -greedy		Success	Failure	Total	1.6×10^{-3}
	Scalpel	71.757	12.593	84.35	
	Photorec	7.841	7.809	15.65	
	Total	79.598	20.402	100	
ϵ -first		Success	Failure	Total	2×10^{-4}
	Scalpel	53.779	9.631	63.41	
	Photorec	18.369	18.221	36.59	
	Total	72.148	27.852	100	
Softmax		Success	Failure	Total	2.4×10^{-4}
	Scalpel	60.428	10.598	71.026	
	Photorec	14.481	14.493	28.974	
	Total	74.909	25.091	100	
UCB1		Success	Failure	Total	7×10^{-4}
	Scalpel	68.348	11.828	80.176	
	Photorec	9.951	9.873	19.824	
	Total	78.299	21.701	100	
Randomization		Success	Failure	Total	1.9×10^{-4}
	Scalpel	42.526	7.397	49.923	
	Photorec	25.175	24.902	50.077	
	Total	67.701	32.299	100	



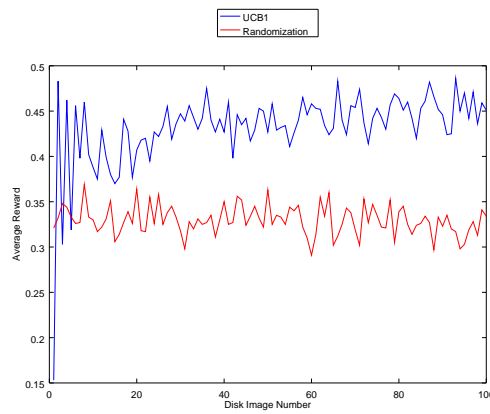
(a) Epsilon Greedy



(b) Epsilon First

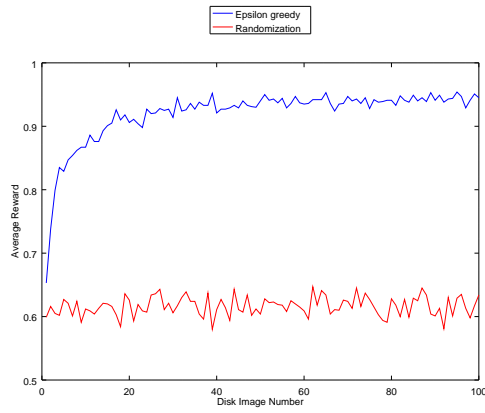


(c) Softmax

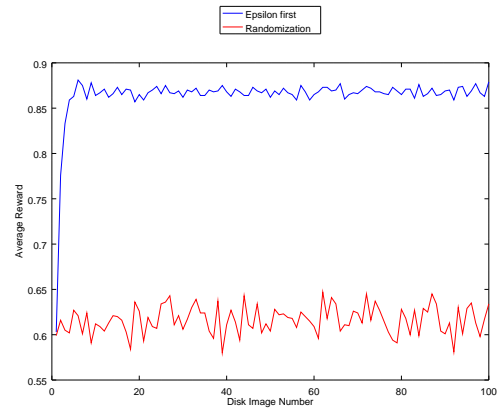


(d) UCB1

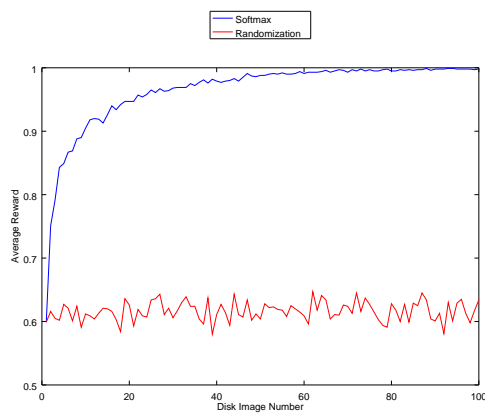
Figure 1: Average reward per disk image over 1000 simulations in the equal sensitive case



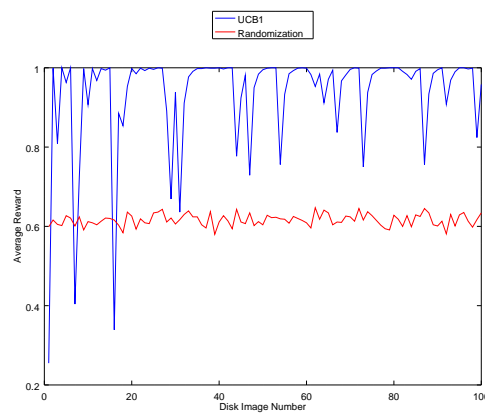
(a) Epsilon Greedy



(b) Epsilon First

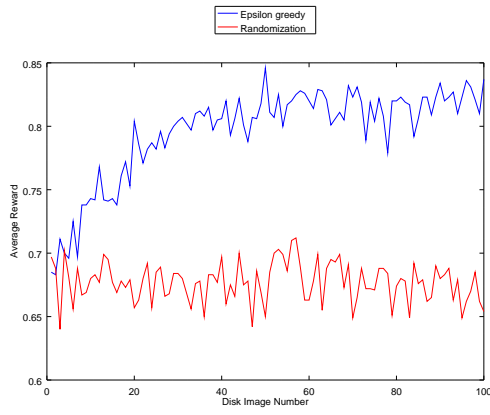


(c) Softmax

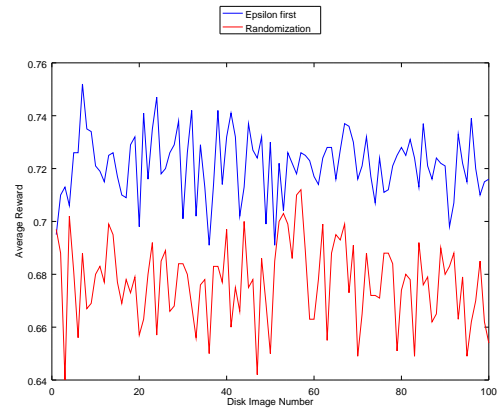


(d) UCB1

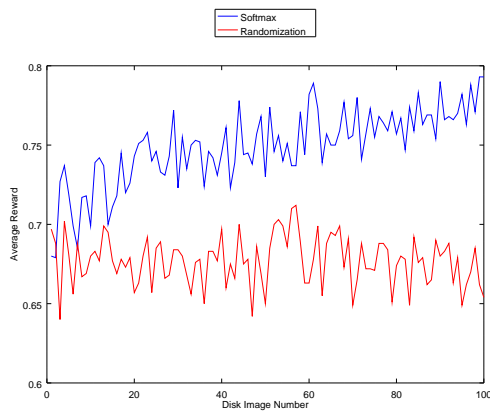
Figure 2: Average reward per disk image over 1000 simulations in the time sensitive case



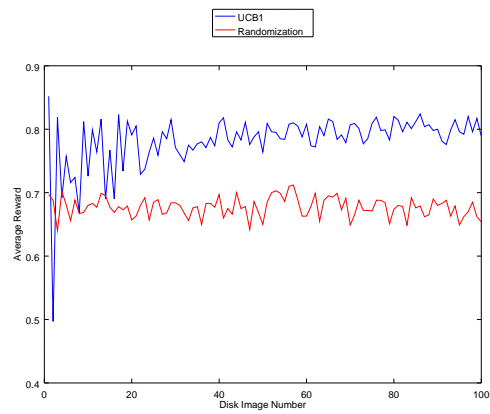
(a) Epsilon Greedy



(b) Epsilon First



(c) Softmax



(d) UCB1

Figure 3: Average reward per disk image over 1000 simulations in the file sensitive case

lem may also be embedded for the purpose of providing learning to artificial intelligence supported tools such as (Hoelz, Ralha, & Geeverghese, 2009; Case, Cristina, Marziale, Richard, & Rousev, 2008; Karabiyik & Aggarwal, 2014; ArxSys, 2017).

ACKNOWLEDGMENT

This work is supported by Faculty Research Grant at Sam Houston State University, Huntsville, Texas, USA.

REFERENCES

- ArxSys. (2017). *Digital forensics framework*. [online].<http://www.digital-forensic.org>. Retrieved from <http://www.digital-forensic.org>
- Auer, P., Cesa-Bianchi, N., & Fischer, P. (2002). Finite-time analysis of the multiarmed bandit problem. *Machine learning*, 47(2-3), 235–256.
- Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. In G. Peterson & S. Sheno (Eds.), *Advances in digital forensics v* (Vol. 306, p. 17-36). Springer Boston. (10.1007/978-3-642-04155-6_2)
- Berry, D. A., & Fristedt, B. (1985). *Bandit Problems: Sequential Allocation of Experiments (Monographs on Statistics and Applied Probability (Population and Community Biology (Chapman & Hall))* (1st ed.). Springer. Hardcover.
- Case, A., Cristina, A., Marziale, L., Richard, G. G., & Roussev, V. (2008). Face: Automated digital evidence discovery and correlation. *Digital Investigation*, 5, Supplement(0), S65 - S75. (The Proceedings of the Eighth Annual {DFRWS} Conference)
- Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation*, 6, S2–S11.
- Gittins, J. C., & Whittle, P. (1989). *Multi-armed bandit allocation indices*. Chichester: J. Wiley. Retrieved from <http://opac.inria.fr/record=b108041>Press, W. H. (2009). Bandit solutions provide unified ethical models for randomized clinical trials and comparative effectiveness research.
- Hoelz, B. W. P., Ralha, C. G., & Geeverghese, R. (2009). Artificial intelligence applied to computer forensics. In *Proceedings of the 2009 acm symposium on applied computing* (pp. 883–888). New York, NY, USA: ACM. doi: 10.1145/1529282.1529471
- Karabiyik, U., & Aggarwal, S. (2014). Audit: Automated disk investigation toolkit. *JDFSL*, 9(2), 129–144.
- Karabiyik, U., & Aggarwal, S. (2016). Advanced automated disk investigation toolkit. In *Ifip international conference on digital forensics* (pp. 379–396).
- Kuleshov, V., & Precup, D. (2014). Algorithms for multi-armed bandit problems. *arXiv preprint arXiv:1402.6028*.
- Li, M., Yang, D., Lin, J., & Tang, J. (2016). Specwatch: Adversarial spectrum usage monitoring in crns with unknown statistics. In *Computer communications, iee infocom 2016-the 35th annual iee international conference on* (pp. 1–9).
- Lu, T., Pál, D., & Pál, M. (2009). *Showing relevant ads via context multi-armed bandits* (Tech. Rep.). Tech. rep.
- Lu, T., Pál, D., & Pál, M. (2010). Contextual multi-armed bandits. In *International conference on artificial intelligence and statistics* (pp. 485–492).
- Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to computer forensics and investigations* (5th ed.). Boston, MA, United States: Course Technology Press.

- Proceedings of the National Academy of Sciences*, 106(52), 22387–22392.
- Richard, G. G., & Marziale, L. (2017). *Scalpel*. [online].
<https://github.com/sleuthkit/scalpel>.
- Sutton, R. S., & Barto, A. G. (1998). *Introduction to reinforcement learning* (1st ed.). Cambridge, MA, USA: MIT Press.
- Vermorel, J., & Mohri, M. (2005). Multi-armed bandit algorithms and empirical evaluation. In *European conference on machine learning* (pp. 437–448).
- Visti, H. (2017). *Forge forensic test image generator*. [online].
<https://github.com/hannuvisti/forge>.
- Weber, R., et al. (1992). On the gittins index for multiarmed bandits. *The Annals of Applied Probability*, 2(4), 1024–1033.
- White, J. M. (2013). *Bandit algorithms for website optimization* (1st ed.). O'REILLY.
- Xu, J., Wang, Q., Jin, R., Zeng, K., & Liu, M. (2014). Secondary user data capturing for cognitive radio network forensics under capturing uncertainty. In *Military communications conference (milcom), 2014 ieee* (pp. 935–941).
- Yi, S., Zeng, K., & Xu, J. (2012). Secondary user monitoring in unslotted cognitive radio networks with unknown models. In *Wireless algorithms, systems, and applications* (pp. 648–659). Springer.

