International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Susceptible Evidence Processing Framework for Handheld Devices Through Digital Forensic Measurements

T. M. Bhraguram[1], Dr. P. S. Rajakumar[2], Dr. N. Kanya[3]

Submitted: 23/12/2023 **Revised**: 29/01/2024 **Accepted**: 07/02/2024

Abstract: Digital forensic comprises various actions for processing digital evidences like preprocess, identification, modeling, extraction, and documentation. All these actions are modelled and entitled through the court of law. Different procedures and methods are followed to perform these actions by the help of various platforms and hardware specifications. The analysis and processing of digital evidences depends on the hardware specifications of various companies and the systematic approach of various effective evidence processing software tools. Most of the hardware developing companies takes the security measures through on board circuits and this helps the digital investigators an advantage while retrieving evidences. Latest technological advancements in industry demands various sensitive security measures needs to be considered while launching new hardware devices specifically for communication purposes. Digital forensic plays a great role in retrieving sensitive evidences and its processing while a digital crime scene is evaluating. This activity considers various processing steps and it leads to the evaluation of both hardware and software participated in the crime scene. Mobile devices are the most sensitive and popular handheld devices used around the globe and the communication capability of these handheld devices makes the message passing and content delivery more flexible hence may lead to the misuse and hacked through the personal space. This article gives an effective framework for analysis and processing of digital evidences specifically for handheld devices like Mobiles, pager, laptop, Notebook and other electronic pads. Nowadays most of the communications occurred through handheld devices so the application of digital forensic measurements on these cases are highly important and sensitive. The digital crime analysis and its effective processing solved by the proposed framework and it integrates various levels of security pads. The framework proposed here comprises LR based Numerical and Verbal likelihood ratio during the digital evidence processing scenarios. This integrated mechanism works on the device platform scrutinize both platform dependent and independent factors and applied on the kernel layer with certain security measurements. Any handheld or mobile platforms may adapt with the changes and the retrieved kernel resources including any suspected communications can pass through the framework channel. Thus the scalable platforms may arise with sustainable security enhancements which are entitles according to the procedure established by law.

Categories and Subject Descriptors

[Digital Forensic Investigation and Handheld devices]: Evidence processing- *Categorization and labelling*.

General terms*: Digital Forensics, Handheld devices, digital evidence*

Index Terms: *Investigation Analysis, processing suite, Likelihood, Digital forensic analysis*

Key words: *Evidence processing, Digital Forensic Investigation, evidence labelling, KDE*

1. Introduction

THIS Article looks forward to establish a sustainable evidence processing mechanism especially for handheld devices. The framework proposed in this article provides an optimal solution which can integrate with the platform kernel of any handheld devices. Most of the mobile or handheld platforms including Apple IoS, Google Android, Tizen OS, Blackberry OS, Symbian OS, Harmony OS, Linux based and Windows OS taking necessary security measurements to prevent the external attacks. As today's technological world is expanding with more technical aspects and security measurements, new security threats and digital crimes also arises. Though leading mobile platforms and tools are bundled with latest security patches and other measurements, still the digital crime and attacks spreading easily with new hacked communications and methods. The forensic device context based on the platforms and the investigations regulates under investigation tools and process models. Various transitions happened under the process models directs the identification of threats and IP spoofing [1][7] which revealed the activities and tasks on a particular time frame. The essential requirements of the proposed framework highly owing the high connectivity demands and communications in out fast growing industry. The Internet of Things (IoT) [3][5][9] filed showing a fast on demand

[1]*Research scholar, Computer Science and Engineering department, Dr. MGR Educational and Research Institute Chennai.*
[2]*Professor, Computer Science and Engineering department, Dr. MGR Educational and Research Institute Chennai.*
[3]*Professor, Head of The department IT, Dr. MGR Educational and Research Institute Chennai.*
Corresponding author: T M Bhraguram (e-mail: bhruguram@gmail.com).

device connectivity and it introduced various sensor and device modules as per the user requirements.

Current research trends lagging behind the perfect evidence collection and its processing for handheld devices and to explore the professional investigation processes for digital forensics. Thus it became a complex discipline and mobile devices interconnectivity standardize the digitalization in a systematic way. The investigation and digital evidence processing is much different from other digital devices than handheld devices. The up-to-date data transmission rate is higher than the classical devices or any other digital devices like desktops.

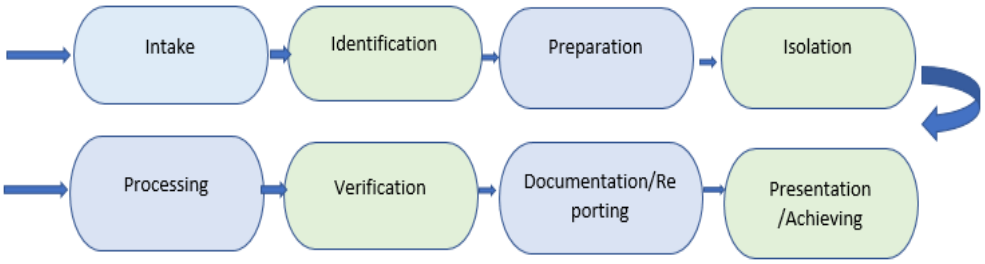

Fig 1: Handheld evidence extraction process

The extraction process incorporates with the framework strategy propped in this article and it progresses according to the calculation possibilities. According to the extraction process the Intake phase always takes the requester seeking content in the form of documentation including the custodial information. All the devices in involved in the investigations are recorded with its features and the document clarifications should be places on the top of investigator goal. Every device and case identification the examiner or the investigator must go through or clarify certain goals which includes the following.

- The authority takes the legal contract of the devices.
- Ultimate aim of the investigation
- The device specification and configuration.
- Device properties like manufacture details and the portable modes.
- Other possible potential evidence modes.

The above goals ae the basic needs and it gives a binding circle during the entire investigation process. Legal authority makes the device examining in more viable way prior to the device contract information placed. The device examination consent is still valid and any possible limitations applicable must be void according the procedure established by law. Examination aim should be clearly specified with law enforcement and it must be regenerated and posted in every phase. Even though the device specifications are easily retrievable, the configuration of various companies and their platforms are different. The examination strategy should be different in such cases which can be applied during the case history evaluation. Device manufacturing companies put certain IMEI (International Mobile Equipment Identity) [4][5][8] for their models and may post the information of portability on the system specification page. The devices with potential threat monitoring sequence and modes can be examined with the legal contract with the companies audit policies.

System preparation makes the system more flexible with the certain goals and criterion already applied on the framework. The criterion includes the possible changes during the investigation time and mode of operation. Some complex device setup anticipated a detailed examination rules which can be settled down with the algorithmic models proposed in this article. Isolation phase highly concentrate on the device technology and its communication mechanism to be investigated thoroughly and it prevents the addition of new data to the device including calls or messages. The remote data destruction also applicable during this time and it accomplished through the use of some radio frequency shield covers or faraday bags. Any accidental overwriting may prevent and initiate a kill signal mode while moving it. The processing part of this framework can reach to te evidence processing effectively by the help of LR [6][7][12][16]based Numerical and Verbal likelihood ratio [2][4][10] and it gives the highest possible evidence evaluation mode before moving to the verification phase. All the processed evidences are verified successfully with the pattern recognition method applied in the pseudocode and the verified evidences reported with documentation form. The presentation phase can execute the decision making part and the extracted reports are archived.

Various tools available for examining the evidences with the technological aspects of handheld devices like GSM, CDMA, iDEN, SIM cards [12][14][18][21]etc. The compatibility of these technologies shown below with logical and physical dump modes. Kessler in 2010 provided this with the tools compatibility and its device support. Remote device extraction and the applicability reached with various categories and modules.

Table 1: handheld device tools feature matrix (Kessler 2010) Modified 2022

	CDMA	GSM	iDen	SIM	Logical Dump	Physical Dump
BitPim	×				×	
Data Pilot Secure View 3	×	×				
Paraben Device Seizure	×	×	×	×	×	×
SIMCon						
iDen Media Manager				×		×
Manufacturer/Other			×			
Cellebrite	×	×	×	×		
CellDEK	×	×	×	×	×	×
Oxygen Forensic Suite	×	×		×	×	×
XRY/XACT	×	×	×	×	×	×
Aceso						
Belkasoft	×	×				×
FinalMobile	×		×			
Simis				×		
Neutrino				×	×	×
ADF DeiPro	×	×	×	×		
ADF TINVPro			×			
Nmap		×				×
SleuthKit	×		×	×		
Sift	×			×	×	
Volatility		×			×	×
MVT		×	×			
Autopsy	×					
Faw		×	×	×		
NFI Defraser	×	×	×	×		
Exif Tools		×	×		×	×
Dumpzilla	×	×				
Xplico	×	×	×	×	×	
CrowsResponse		×	×			×

The latest tools descriptions modified and included with the features support. The parameters considered for each tools got different during the investigation time and most of these helped to collect the evidences and analyze it with the comparative features already in the database. Hence these models navigate with certain feature selection and comparison operations, the case characteristics may deviate with case by case. The study on these tools understand the

analysis models but most of the cases, the evidence processing cannot exceed the sufficient level of accuracy. The accuracy measurements are normalized and optimized for the result parameters. The existing tools may consider the processing strategy in local mode though they cannot handle the remote evidence collection and its processing criteria.

Instead the direct feature selection, the framework proposed here can formulate the evidence history with the calculated possible ratio which lead to the direct impact on the accuracy and the modified evidence part. The framework here may take multiple iterative steps of evidence handling and the portable decision making tool can deport with any existing forensic tools. The system developed based on the tool leveling structure proposed by Sam brothers in 2009. According to the structure we need various level of dumps including manual extraction, Logical analysis, Hex dump, Chip Off and Micro read [16][14][5][4]. All the physical level examinations made through the examiner and the extracted evidences are kept hided with maximum security. A level of PGP (Pretty good privacy) [22][7] encryption standard is suggested to do this and the logical phases are running with the algorithmic flow proposed under this framework. Manual extraction process involves the normal handheld device content extracted manually by scrolling the contents and documented it through photographic measurements. Devices keypad or touchscreen enabled for this process and its easy and fast and can be applied to almost all handheld devices. This process prone to error due to the unfamiliarity of device interface and leads to the misreporting of critical evidence content.

Logical extraction performed by connecting the device to the forensic hardware or workstation by means of USB cable or RJ-45 cable, [11][13][15] Bluetooth or infrared. After a successful connection the system imitates a command and send it to the device which is then interpreted by the processor of connected device and the requested data send to the workstation. After receiving the evidence from the device the processing happened through ten algorithmic ratio proposed here and the examiner can review it with various extracted results from the algorithm. Delete the evidence content is inaccessible and the examiner doesn't need any experience on this process.

Hex Dump is the process of physical extraction and the operation is achieved by pushing the unsigned code or a bootloader into the phone after connecting it. Its instruct the device to dump the memory to the system. The result extracted is in the form of Binary Raw image, a technical expert is necessary to analyze it. The cost effective process provides sufficient data to the examiner and also its allows to recover the deleted files from the unallocated spaces.

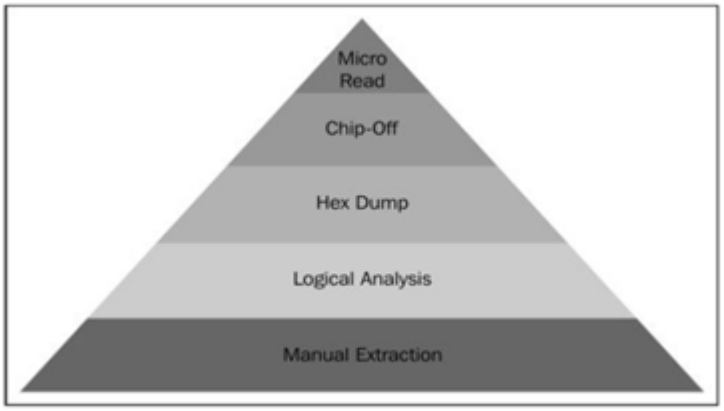

Fig 2: Handheld Tool leveling structure (Sam Brothers, 2009)

The most sensitive data acquisition part happened under the Chip Off level and it recovers the data directly form the device chip. The device chip needs to remove physically and by the help of chip reader or with a new processor device the data can be recovered. A technically challenging task as this phase is suffered by the chip categories produced by different companies. An expert with hardware knowledge is necessary and an expensive task and any improper procedure may lead to the chip damage. The chip detachment is a careful task and it should have done by taking necessary measurements. All other extraction levels must be tried before concentrating on this level. The destructive nature of this level is more sensitive and necessary training expected to do this. The parsing of the retrieved data content is necessary as the resultant data coming from the level is in raw manner. The operation in this level is normally done through Joint Test Action Group (JTAG) method. This operation involves the connection through Test access ports (TAPs) [17][19][20] and instructing the processor to transfer the data. When the device is inaccessible and cannot access through standard tools, then this strategy is applicable.

Micro read process performed manually by viewing and parsing the data directly from the chip. The examiner used an electronic microscope and review the physical gates on the chip and then changing the gate status to 0's and 1's to obtain the resulting ASCII characters. Costly and time consuming task also demanding the expert knowledge about the file systems and flash memory. This level is

attempted only in high profiled cases as it requires more technical expertise. This level is only applicable in high security threat cases where any other evidence collecting level exhausted.

2. Related Works

A detailed logical acquisition and analysis of data from android mobile devices proposed by the authors (Himanshu, 2015) makes the knowledge regarding the android route map its data retrieval. The solution proposed uses the identical problems and its similarity searches to retrieve the evidence and has the limitation of platform independency. The solution tried to move the data acquisition part into steady stage and the crunched data collected to be used for analysis and may result into the mode of timely constraints. Expected the analyzed data to be interrelated and it must correlate with any of the adaptive tool [2].

In 2011, Lai Y and Yang C proposed a forensic tool for android smartphones and the article proposed this system specifically through cloud bases system. The evidence extraction and processing done through similarity search models and the raw evidence processing strategy not defined with modified information. The system may perform a single round evaluation for the sensitive data and the data managed through cloud based platform [7].

A security solution for android mobile forensics developed by Kubi et al., 2011; Saleem et al., 2014, 2013; Saleem & Popov, 2013) and proposed methods for selecting the tools to integrate. The technical aspects in this article makes the system uses various criteria to be evaluated while selecting the forensic tool. The security challenge presented as the important criteria and the system is based on the NIST specifications [5].

(Bonnington C. Wired in 2015) suggested an evaluation of forensic methodologies which are capable of handing the forensic issues. Both ISO/IEC and NIST methodologies are failed to handle all the forensic issues found till the year and for some non-technical problems ISO/IEC is advantageous [4].

The disk capability and its sates are seriously evaluated by (Regan, 2009) and got the solution of disk architecture and its platters property where the handheld devices fall under. The slid state drives used with handheld devices are smooth and adaptable for the devices due to non-moving parts character and the ease of analyses. These are susceptible to shake damage as it doesn't provide any moving device parts [9].

The article published by (I. Riadi and A. Firdonsyah) regarding the forensic investigation technique focused on devices which are running under android based platform. They want to emphasize the investigation process and then comparing the necessary tools based on the NIST framework (National Institute of Standard and Technology. They used 4 different forensic tools to examine the android devices and the performance are measured quantitatively [11].

S. Saleem, O. Popov, and I. Baggili, 2016) suggests the decision method through performance of the evaluation and the parameters based on the hypothesis. All the hypothesis applicable on forensic method and tools evaluation. The particle suggest freedom of choice necessitates theory. This is the sense of responsibility which asks the Boolean expression true/false criteria [4].

A Score-based likelihood ratios for handwriting evidence published by Hepler AP, Saunders CP, Davis LJ, Buscaglia J (2012) expressed the possibilities range specifically for handwriting evidences and this can be used as a tool as integration modules. The more likelihood ratio applied and the Bayesian possibilities are recorded with the evidence hypothesis and performed the conditioning constraints more adaptable to the graph axis. This become one of the effective evidence processing strategy for handwritten contents [6].

Confidence intervals for the ratio of two binomial proportions suggested by Koopman PAR (1984) was the basic proportions model adapted for various binomial possibilities. Here the standard ratio taken as the nominal parameter and the iterative steps performed with each data occurrence with specific intervals. This method applicable in various forensic tools as the basic model proportions to find the best ratio for the evidences collected by various mediums [17].

Variation in Likelihood Ratios for forensic evidence evaluation of XTC tablets comparison proposed by Bolck A and Alberink I (2011) analysed the variations and its drastic deviations once the likelihood ratio is applied. The Bayesian theorem formulated according to the sensible and cleansed data content. The XTC based table comparisons made available to the likelihood ratios and the variations are recorded in each phase of evaluation [12].

Data analysis in forensic science- A Bayesian decision perspective proposed by Taroni F, Bozza S, Biedermann A, Garbolino P and Aitken CGG (2010) had given a good data analysis technique especially applied for digital evidences and based on Bayesian perspective. This method collage with the likelihood ratio become the most sensitive data analysis part and pave the way for many digital crime investigations. The probabilistic decision making happened over the test data is iterative and the hypothesis applied in each level of execution falls under three possibility ranges and become the necessary path to the decision making [13]

3. Materials and Method

The Likelihood ratio is the direct approach of Bayes rule/theorem and was developed by English clergyman

Reverend Thomas Bayes (Bayes & Price, 1763) in 18th century. This can be represented in terms of ratio of possibilities called odds. In digital forensic we adopted LR approach with the ratio of possibilities of two hypotheses (say H_p and H_d) and this case considered before finding any certain similarities. The evidence is represented as E and considered into account called prior odds and after the evidence known it may be represented as posterior odds. The hypotheses always take two sides like positive determination (H_p) and negative determination (H_d) though this is not always the case. The Bayes rule is always shows the probabilities changes due to the findings: -

$$prior\ odds \times Likelihood\ Ratio = posterior\ odds$$

For the ease of notation explicit mentioning of the background information I is omitted here. This information is assumed known in all probabilities.

in odds terms:

$$\underbrace{\frac{P(\mathrm{H_p})}{P(H_d)}}_{prior\ odds} \times \underbrace{\frac{P(E \mid H_p)}{P(E \mid H_d)}}_{LR} = \underbrace{\frac{P(H_p \mid E)}{P(H_d \mid E)}}_{posterior\ odds}$$

(1)

A)Numerical Likelihood Ratios

In most of the digital forensic fields (eg: content misuse, wrong posting, spoofing, data drop, hacking, calls hijack, Fine tune analysis) LR models explicitly used to calculate numerical values where the possible ranges fall under. The developments and construction of models for calculating numerical LR applies standard likelihood ratio possibilities and the comparison criteria based on the hypothesis.

a.1 Distribution of univariate discrete characteristics

When a bunch of possible evidences considered as the highest possibility ratio, certain univariate discrete characteristics must be considered and the query related to the posterior probability to measure the strength of the evidence. Some forensic experts can provide the solution of the query related to this probability. Any physical characteristics affects the probability ratio must be separated or combined based on the likelihood ratio and generate corresponding hypotheses. The hypotheses can be formulated as

- H_p: Any evidence bunch of consignments X and Y come from the same devices or same scene where the incident occurred at the same time interval.
- H_d: Any evidence bunch of consignments X and Y come from the different devices or different scene where the incident occurred at different time interval.

Let's consider the *univariate discrete* case, where we will consider just one characteristic (e.g. chip model) that only can have a limited number of values (e.g. IBM or Intel chip models can have limited number of chip set categories). This is very similar to the evidence bunch with probabilities on positive or negative test results. To construct LRs the probabilities on specific univariate characteristics are needed. These probabilities or proportion (π) can be estimated based on the frequencies of univariate characteristics in the evidence bunch that are generated for the case during a particular time period.

If the univariate character of two evidence bunch have the same Chip, this could be considered as a match. This match can be taken as the evidence, but not only the fact *that* the chip model match but also *what type of company chip* match is of importance for the strength of evidence. Therefore, for clarity it is better not to consider the match or non-match as evidence, but the fact that both characteristics are for instance *same company (say IBM)* or one evidence bunch with character *IBM* (x) and the other with a *Intel* (y). The LR then can be written as

$$LR = \frac{P(E \mid H_p)}{P(E \mid H_d)} = \frac{P(X = x, Y = y \mid H_p)}{P(X = x, Y = y \mid H_d)} = \frac{P(Y = y \mid X = x, H_p)}{P(Y = y \mid X = x, H_d)} \times \frac{P(X = x \mid H_p)}{P(X = x \mid H_d)}$$

(2)

This uses the definition from probability theory that $P(X,Y) = P(Y|X)P(X)$, used in the deviation of Bayes rule and earlier in the evidence combination. Last term represents the ratio of the probability of a certain character under the two hypotheses. The probability doesn't consider whether X and Y come from the same evidence bunch or not and always equal under both hypotheses. The ratio is thus assumed as equal to 1. Thus distribution of univariate discrete characteristics as

$$LR = \frac{P(Y = y \mid X = x, H_p)}{P(Y = y \mid H_d)}$$

(3)

The probabilities of the number of certain evidence pair at various bunches are considered, and it is assumed that these are more or less independent. The separate probabilities may be multiplied and combined (with a small correction) to what is known as the match probability. For all independent univariate discrete characteristics, a similar (multivariate) LR model can be used.

a.2 Distribution of multivariate discrete characteristics

When the features are combined or the LR of independent univariate characteristics by the product of LR, then it estimates the features of separate variants. If the characteristics are dependent of each other, sometimes it gets shared the same hypothesis.

A multinomial model with proportions π_i in categories i =1, …..k instead of a binomial model with proportion π in the univariate case can be assumed.

$$f(x_1, x_2, \ldots, x_k) = \frac{n!}{x_1! x_2! \ldots x_k!} \pi_1^{x_1} \pi_2^{x_2} \ldots \pi_k^{x_k} \propto \prod_{i=1}^{k} \pi_i^{x_i} \quad (4)$$

with x_i the number of features in a particular category I and $\sum_{i=1}^{k} x_i = n$ the total number of features

a.3 Distribution of univariate continuous characteristics

We need a new LR model specification once the evidence is not discrete but continuous. Continuous data can take all possible values between certain limits of the evidence recap. The basic structure of LR will be same but instead taking discrete probabilities *(P)* continuous probability densities *(f)* used:

$$LR = \frac{f(y \mid x, H_p)}{f(y \mid H_d)} \quad (5)$$

The mean and variance of the distribution can be estimated based on measurements of various evidences of the reference batch (*X*). This determines the distribution of the numerator. The distribution in the denominator can be estimated from the background data (*Z*). Instead of estimating the unknown parameters again priors may be used. In assigning priors one can use the fact that a relation exists between the distribution of individual batches and the whole evidence of batches. The whole evidence batch is the sum of all existing batches.

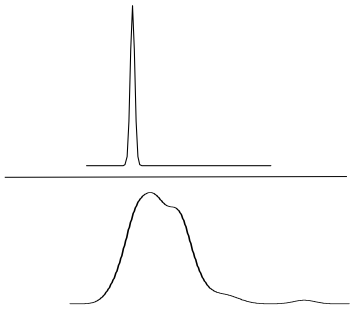

Fig3: Gaussian distribution of Numerical and Experimental Curve

A Gaussian distribution is less indicated. The distribution of overall evidence batch concentrations depends on the manufacturer preferences of hardware or software. There may very well be more than one peak, or the distribution may be very skewed. Other parametric distributions, such as e.g. beta distributions or empirical distributions, such as histograms with methods like Kernel Density Estimation (KDE) [4][5][7][8] may be better options (Aitken and Lucy 2004, Aitken et al, 2007).

Instead of finding the unknown parameter estimation, again priors may be used. Using uniform or conjugate priors or by using external information to construct informative priors can be done through this. While assigning any prior criteria, its explicitly found the fact that there might be relation exists between the distribution of individual batches of evidences and also the whole evidence group. Based on this, Aitken and Lucy (2004) suggested to adapt the above LR model where the mean θ in each evidence batch is assumed to come from a distribution *f(θ)* [3][5][22] representing all possible means in the evidence batch. Ten variance must be assumed as fixed and equally starts with.

The mean distribution can be assumed as the Gaussian or the instance a KDE on the empirical data (Aitken and Lucy 2005), e.g $f(\theta_i) \sim N(\mu_0, {\tau_0}^2)$. The LR can be replaced as follows: -

$$LR = \frac{f(y \mid x, H_p)}{f(y \mid H_d)} = \frac{\int f(y \mid \theta, H_p) f(\theta \mid x, H_p) d\theta}{\int f(y \mid \theta, H_d) f(\theta \mid H_d) d\theta} \quad (6)$$

Where the numerator represents predictive posterior distribution and the denominator indicates the predictive prior distribution. If $f(\theta_i) \sim N(\mu_0, {\tau_0}^2)$ is used as the prior criteria, then we can update the formula with evidence data within the batch to compare with $\bar{x}$ results in the posterior

$$f(\theta \mid \bar{x}) \sim N(\mu_n, \tau_n^2) \text{ with } \mu_n = \frac{\frac{1}{\tau_0^2}\mu_0 + \frac{n_x}{\sigma^2}\bar{x}}{\frac{1}{\tau_0^2} + \frac{n_x}{\sigma^2}} \text{ and } \tau_n^2 = \frac{\tau_0^2 \sigma^2}{\sigma^2 + n_x \tau_0^2} \quad (7)$$

Then the LR becomes more specific in this case and may take the form below for the specific case. This has been proposed by (Block et al 2009). The proposed framework here in this article use this modified LR based module for the distribution of univariate continuous characteristics during the evidence analysis of interrelated evidence batch.

$$LR_{\bar{X},\bar{Y}}(\bar{x},\bar{y}) = \frac{u_0}{u_n}\exp\left(\frac{1}{2}\left(\frac{(\bar{y}-\mu_0)^2}{u_0^2} - \frac{(\bar{y}-\mu_n)^2}{u_n^2}\right)\right) \quad \text{with } u_0^2 = {\tau_0}^2 + \sigma^2/n_y \text{ and } u_n^2 = {\tau_n}^2 + \sigma^2/n_y$$

(8)

Here the normal priority may not be indicated and a no parametric prior on the same data can be used. If the variances differ within evidence batches, it is better to estimate the individual variances within the specific manufacturer group items.

a.4 Distribution of multivariate continuous characteristics

The univariate considered single continuous characteristic for calculating the LR and it can be easily extended to multivariate by considering more than one continuous characteristics at the same time. Dependent characteristics [23] can be considered. Due the similarity of same hypotheses characteristics, a joint distribution for all the combined characteristics can be considered which may change the multivariate densities as follows: -

$$LR = \frac{f(\bar{\mathbf{y}} \mid \bar{\mathbf{x}}, H_p)}{f(\bar{\mathbf{y}} \mid H_d)} \tag{9}$$

Here the numerator dictated as the density of values $\bar{\mathbf{y}}$ of *k* number of characteristics in the device or software manufacturer group where we need to consider the evidences. While in the denominator the *k*-variate distribution of the characteristics in the evidence batch arises with prior on the mean or variance can be taken as:

$$LR = \frac{f(\bar{\mathbf{y}} \mid \bar{\mathbf{x}}, H_p)}{f(\bar{\mathbf{y}} \mid H_d)} = \frac{\int f(\bar{\mathbf{y}} \mid \boldsymbol{\theta}, H_p) f(\boldsymbol{\theta} \mid \bar{\mathbf{x}}, H_p) d\boldsymbol{\theta}}{\int f(\bar{\mathbf{y}} \mid \boldsymbol{\theta}, H_d) f(\boldsymbol{\theta} \mid H_d) d\boldsymbol{\theta}} \tag{10}$$

According to (Weyermann, 2008), priors on the variance can be used for the said transform and the combined form taken in this case can be modified and transformed based on the evidence correlation and relevance on the digital crime scene. A more specific evidence batch may have showed with high prioritized group modification and thus the results become centric among the entire evidence batch. Many variances formulated and presented in recent years as the presented models in this article takes the stable calculations in most of the evidence batches, its adopted in the framework module. Once the Numerical likelihood ratio completed, the same evidence batch may be analysed with distance measurements and similarity scores with same group evidence scores. The possibility of high positive scores slightly deviating while the evidence cleansed area, still the correctness of numerical indicators is relevant for the sufficient evidence group analysis.

a.5 Similarity scores and distance measures possibilities

This numerical method dictates a new approach in using multivariate(dependent) characteristics (either continuous or discrete) to calculate the likelihood ratios based on the score model (Hepler 2012). Here we can use the distribution of calculated distances or similarities between the features. The Pearson correlation distances between characteristics are calculated between two case hypothesis and generate the possible best links as the results. A sufficient number of links can be taken into consideration with respect to Pearson correlation distance and used for the next level of forensic investigation.

The distance measured $\rho = \frac{1-r}{2} \times 100$ where r is the Pearson correlation between any two evidence data. Other distance measurements like Euclidean distance also can also be used as well. In the score based measurements we can perform LR calculation based on the values and distribution of distance (similarity scores) between the characteristics of the evidence under comparison.

The back ground data representation can be used to estimate the distribution distance or scores within the same evidence batch comparisons and also the scores between the different batch comparisons. This may be estimated parametrically or empirically with the Kernel density methods (KDE). The likelihood ratio [4][6][11][12] can be formulated by the comparison of data **x** and **y** always takes the density of the observed distance or similarity measurement (*d*) between the two evidence data content under the two competing hypotheses.

$$LR = \frac{f_w(d(\mathbf{x},\mathbf{y}) \mid H_p)}{f_b(d(\mathbf{x},\mathbf{y}) \mid H_d)}, \text{ with } f_w \text{ the within-distribution and } f_b \text{ the between-distribution.} \tag{11}$$

We can measure the accuracy of these methods more contrast in the sense that it6s falling under theoretical cases. Feature based methods are more suitable for digital evidence evaluation and here the features themselves are the evidence and the probability of the next immediate evidence data. This is applicable once the evidence

estimation or evaluation under two competing hypotheses. The full multivariate structure of the dependent features can be considered and the result produced the height of LR which might be determined by the correlation of the feature values of two or more compared items and the rare occurrence of the features.

B)Verbal Likelihood Ratios

Normally LR approach [3][4][5][9] can be used in many of the digital forensic evidence categories where two or more incidence or retrieved data to be compared and some uncertainty affecting interpretations like IP address, disc structure variation like file system, operating system core affected etc. Due to the forensic expertness lagging, in many cases the forensic person cannot compute the probabilities manually. Then the investigator does this by collecting subjective probabilistic estimation by the existing knowledge, expertise and experience in the same field of study.

Some verbal statements possible to measure the likelihood ratio where two probabilities are compared. Depending on the evidence strength, the following categorization is possible.

The finding falls under: -

- The probabilities are equal
- More chance to probable
- Highly probable
- Very highly probably
- Extreme probable

These categories made under hypotheses 1 and 2

The higher probabilities finding the evidence is falling in one hypothesis than the other, may stronger support of the previous hypothesis. Instead of the categorizations the group is measured with degree values as the verbal interpretations are difficult to conclude.

Table 2: Relate Verbal and numerical LRs (AFSP 2009)

LR Value Range	*Equivalent Verbal form*
More than 1 and up to 10	Weak support of the evidence
From 10 to 100	Moderate support
From 100 to 1000	Medium strong support
From 1000 to 10,000	Strong evidence support
From 10,000 to 1,000,000	Very strong evidence support
More than 1,000,000	Extreme evidence support

These degrees are the magnitude of the likelihood ratio and the ranges represented with corresponding verbal equivalent. The calculated LR value possibilities may deviate from the range of one to 10 lakhs and officially conclude by Nordgaard in 2011.

4. Configuration Profile

The proposed framework combined a various parametric modules and evaluation procedures which are highly sophisticated under surveillance measurements and categorical labels. The content evaluation occurred for every evidence data and the retrieval method accomplished by both manual and systematic approaches. The configured modules attached with this framework running under the evidence retrieval phases and integrate various evaluation procedures. The framework provides both numerical and verbal [3][5][9][13] based evaluation approaches where the investigation experts failed to formulate the statistical evidences. The digital crime scenes are so critical and fast response needed and this immediate and proximal attention gives the best result and it deviates from its real character as time goes on. Here a more detailed evaluation procedure takes place and the results are immediately posted to the corresponding storage container with sufficient archival. The pseudocode below depicts the Micro content evaluation procedure with its chip detachment. The framework is more confident to profile its characteristics and code with accuracy. As the micro content retrieval and evaluation is a sensitive procedure, here it collects the method to accomplish the task with a zoomed mode.

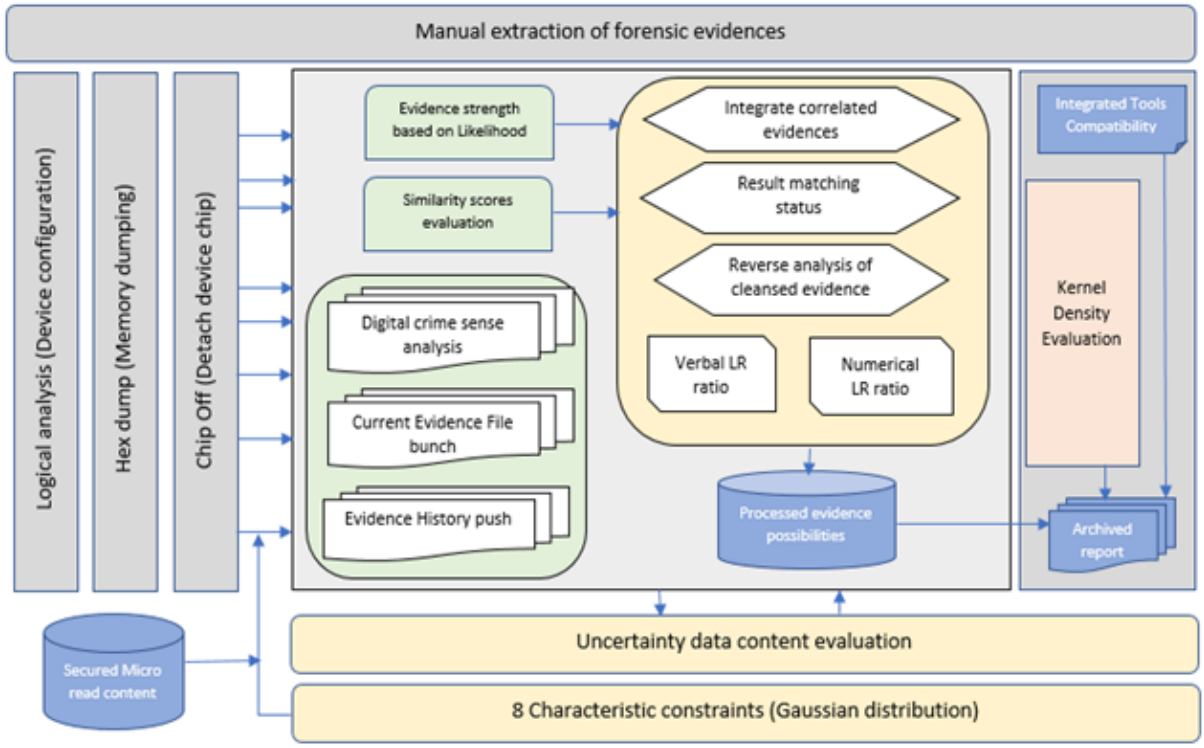

Fig 4: HldRootKit forensic evidence processing framework

System depicted here controls a large component module and its operations with sub modules produce the results with Numerical exact and verbal degrees. This concept overcome the difficulties during the evidence evaluation with different categorical data. HldRootkit evaluation framework maintains two base containers serves as the storage modules where the system can hold both sensitive and root map data. All the required evidence possibility contents can be pushed here with certain security measures. Manual evidence extraction can perform parallel with other expertise or system evaluation but the pushed contents action should be consolidated one which cannot rollback once the evaluation process started. All the device configuration details must be recorded and indexed for the content label matching [5][7][24] purpose and this logical analysis module can be rerun to obtain the labels with at least 60% accuracy. This must be ensured by the help of company profiles of the device manufactures and the domain expert.

A successful logical analysis leads to a hexdump procedure where the memory contents retrieval is possible and all the sensible and generic contents might be recorded and transferred to the destination system where the possible framework optimization is done. Hexdump can be iterated a limited number of times and rerun possible with new parameters or evidence criteria. The memory contents must be recorded according to the conversion mechanism and the corresponding hash code will be generated before transmitting to the destination system to ensure the maximum security.

Device chip off mechanism [4][6][9] initiated for micro read contents and may take proper security measures and care while detaching the chip and also during the evidence extraction. Secured storage container expected to store the most sensitive data and the process takes longer time as this need more expertise and other equipment suitable to detach the physical part and retrieve the contents. This process may rerun with manual experts and equipment most suitable for the retrieval and detachment. The output from logical and Hex dump may use in this step to make the process running smoothly and to save the time.

```
Initiate Device configuration map
<Configure device label, IMEI split up>
        ! Image code reciprocal, !Storage status and mode
<File system mapping, Event check>>
<Steam mantle>
 ! Chip displacement <Damage note written>
 ! Retrieval percentage written
 ! Committed
 ! Chip detach completed
<Stream mantle fixed>
<Rollback>
        <Set Mode of retrieval and Percentage callback>
        <Loop evidence retrieval continue to 3 attempt>
                <First attempt of retrieval 40% callback>
                ! Initiate root cause and Device address
                $ Init value 1 $
                $ Find the labels $
                $ jump to next address point $
                  $ Look back for previous address saved $
                $ Complete the steps up to last control block $
                $ Write back the resultant retrieval $
                $ Interpret the retrieval mode $
                $ Commit it $
         <Loop Exit with status code>
        & check the status code &
        & status recognized True or Boolean expression score greater
than 1 &
                        <Retrieval status- completed with satisfactory level>
        & else &
                        <Retrieval failed and recorded below threshold>
                       <Roll back for next set of attempts>
```

Table 3: Procedural pseudocode of Micro read content

Micro read of the specified chips include various of labelling operation and identifications. Its anticipated to produce the steps to be iterated once the retrieval mode changed without any status code and also once its reached threshold retrieval level. A rollback operation suggested during this time and multiple steps to be iterated once its moved without any satisfactory evidence content. Each address point of the device chip to be examined and the intermediate address labels to be stored to make the smooth flow of the retrieval process.

This sophisticated content retrieval is sensitive and must coordinate under the expert direction. The status code indicates the level of satisfied content and based on this status, a rerun must be initiated with more adversary. One of the crucial part of the framework where the manual experts and system time to be spent to complete the evaluation is Micro content read[3][4]. As most of the micro content read and evaluation procedures fails, the framework suggests rerun up to the maximum optimized result to be generated. The transfer process must be secured one as the sensitive data flow may fall under packet drop while transferring. This content read procedure strengthen the framework as developed here and the support of the retrieval evidence solved around 50% of the case evaluation.

The core of the framework concentrates more on the evidence strength based on likelihood ratio calculation. A more effective similarity scores measured with the likelihood ratio can be distributed towards the result matching criteria where a more detailed criteria evaluation happened with integrated correlated evidences. The cleansed evidences undergone for reverse analysis and the verbal numerical LR calculation made. This step qualifies the content matching process with minimal round of execution and the possibilities pumped to the secured container. The final archived report might be disseminated with KDE histogram [4][5][7][15] combined model and other external tools integration if needed. The below pseudocode represents the NVLR processing [5][7][11][12] strategy used in the framework during the content matching and label assigning.

```
Declare the hypothesis content and possibility ratios ranges
Push the univariate discrete characteristics mode
      <Chip content match>
      <Apply the possibility ratio>
      <Device manufactures labels>
   <if ratio match and chip content>
      <same category: strong match degree found>
      <same category but labels not found: push the content to categorical match
      <different category: match degree not found>
      <different category but labels found: skip to the next degree of occurrence>
   <Write back the contents and commit it>
   <Misinterpretation detected: Rollback and initiate the variables again>
Push the multivariate discrete characteristics mode
   <Combined category labels checked>
      Multinomial model or proportions found: combine all the features
      Else
      Process it with separate categorical labels.
Push the univariate continuous characteristics mode
   <distribution coefficient declared>
      $ Find the Gaussian distribution $
      $ Numerical curve to be formed for categorical elements $
      $ Find the mean distribution and predictive posterior $
<Write back the contents and commit it>
<Misinterpretation detected: Rollback and initiate the variables again>
Push the multivariate continuous characteristics mode
   < Combine multiple univariate continuous characteristics>
      $ Do joint distribution $
      $ calculate densities of the selected features $
! Initiate similarity score finding and possibility measure
Join the verbal LR range degrees
Conclude with hypotheses equivalent form
```

Table 4: NVLR Processing pseudocode

The Numeric and Verbal likelihood ratio [4][5][7][12]module remains in this framework carries multiple evidences files to initiate various content matching operations. The evidence processing considered both numerical level possibilities and verbal degrees to complete the content matching and labelling. The hypothesis used in this model must be initiated with possible range values and the operation performed with 4 numerical range calculations and one verbal degree. The numerical range calculations fall under univariate discrete characteristics mode, multivariate discrete, univariate continuous and multivariate continuous modes.

Micro content chip label matching done with possibility ratio and device manufactures label. It falls under 4 categories after checking the ratio match and chip content. If this falls under same categorical label, then a strong match degree found status has been reported.

In case the matching criteria falls under same category but with no labels, a content push might be initiated to categorical match. If it's with different category, match degree status not found and the same will be committed to the storage container or secured database attached. The last category falls with different category reported but labels found means the system must skip to the next degree of occurrence.

Every operation status committed with the write back labels and contents and any misinterpretations of the categorical labels a rollback must be initiated with all the variables status to null. The above operation considered the evidence file lean mostly to the univariate discrete characteristics mode. Multivariate discrete characteristics mode is different with operation status as this mode combined various categorical labels and checked its multivariable characters. Once checked out of its proportions, the integral operation triggered otherwise a separate processing operation done with each categorical labels.

During univariate continuous characteristics [3][6][7] processing a coefficient declared for distributed characteristics labels. Histogram combined Gaussian distribution labelled and corresponding numerical curve to be formed for each categorical elements. The calculated mean distribution and predictive posterior values are committed with labelled contents. Any misinterpretations are rollback and initiate all the variables again as like univariate discrete mode.

When u have a multivariate continuous combination [3][6][7] , a sum of all the labels are needed and the combination may be used with joint distribution operation. The densities might be calculated only for the selected features. Similarity scores and possibility measures done after all the labelling processes with successful integration

of verbal LR range degrees. A concluded hypothesis equivalent form to be disseminated to the secured container for further integration of third party tools if required.

```
density (variable x, variable qw = "nrd0", adjust = 1,
            Kernel  = c("gaussian", "epanechnikov", "rectangular",
             "triangular", "biweight",
             "cosine", "optcosine"),
            Weights = NULL, window = kernel,width,
            Give.Rmode(Rkern) = FALSE, subdensity = FALSE,
            n = 512 from, to, cut = 3, na.rm = FALSE,...)
plot(Rmode value)
calc_bandwidth()
double cdf(double x, double y)
double cdf(vector<double>& data)
double get_bandwidth(int x){return(bandwidth_map[x])
int get_vars_count(){return(data_matrix.size())
```

Table 5: Kernel Density Evaluation (KDE) procedure in R statistical analysis

A histogram based kernel density evaluation (KDE) [4][5][8] apt for the distribution label representation after the evaluation procedure. The model to be used as the decision making tool after the successful integration of third party evidence files or tools if required and the KDE procedure implemented under R statistical analysis. Various kernel models can be initialized including gaussian and biweight. The statistical programming code attached in this article gives the bandwidth mapping structure and the evidence data matrix to be mapped with labels count.

5. Results and Discussions

The normal distribution of likelihood ratio represented in gaussian histogram can reveal the statistical results of the evidence processing. The digital evidence analysis performed through this Gaussian distribution depends on the numerical and verbal LR deviate its curves slightly towards the density measures in case the evidence category mismatched with its history contents. Both feature based and score based results shows the evidence categorization and its label assigning done through the various LR degree values where multiple categorical values processed at the same time. Whenever the feature selection depends on the batch number, the categorical deviation decreased according to the ups and down deviation of evidence content. As depicted in the graphs, the feature based categorical labels always distributed among the maximum LR variations [3][10[19] but score based increased its deviation in normal mode. The possibility values range is static in most of the cases when we consider score based as it gives the labelling process easy for evidence batch.

The below depicted histogram specifications give the static and dynamic deviation of evidence data., where we considered both feature based and score based models. The result shows that the evaluation mechanism used in the framework illuminates all the possible feature selections collected through various extraction methods.

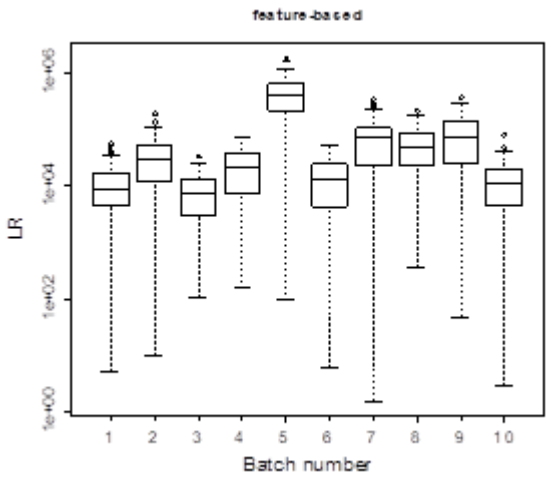

Fig 5: Feature based LR labelling

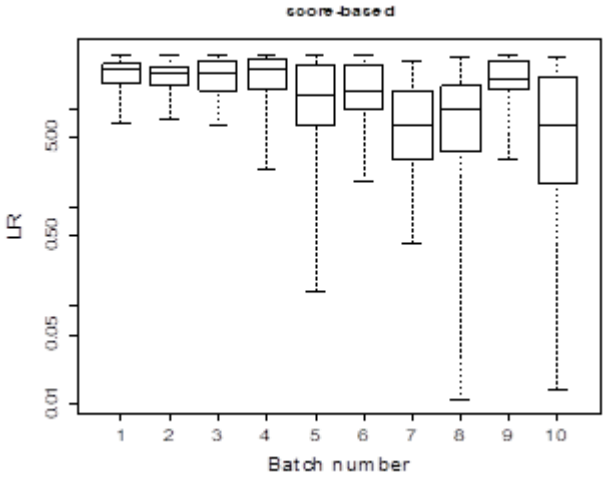

Fig 6: Score based LR labelling

As per the standards likelihood positive and negative level calculations the framework results deviate its categorical label based on the maximum likelihood ratio [5][9][11[13]. The calculations for positive sensitivity below takes the order category which may always lean to the positive region where we can assign the possibility values of a specified evidence data is strong. The negative sensitivity model calculates the prior divisions where the possibility range falls under the non-matching data category.

The positive and negative LR sensitivity calculations performed with the equations below and its integrated to the univariate or multivariate categorical label according to the classified contents.

LR+ = sensitivity/1 – specificity LR + = Pr (T+ | D+) / Pr (T+ | D-) (12)

LR- = 1 - sensitivity/specificity LR - = Pr (T- | D+) / Pr (T- | D-) (13)

Based on the LR possibility ratio [6][7] deviation the histogram plotted represents the evidence strength can become the highest possibility contents and this might be censored and routed to the next batch of evidence processing.

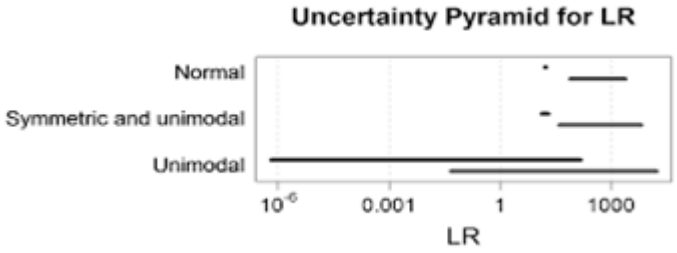

Fig 7: Uncertainty evidence data plot

The cumulative results of all evidence batch processed shows the likelihood ratio calculated in the proposed framework strengthen the evidence module and it considered all the possibility range values. The range values met with certain curve where we can find the cumulative proportion modulates the evidence category and the exact labeling happened without any rerun in most of the cases.

The cumulative proportion ranges the values from 0 to 1 for positive measurements and likelihood ration take both negative and positive ranges where the maximum likelihood values fall under. The range of -10 to +5 values of likelihood is sufficient to categorize all the evidence group processing with its corresponding label.

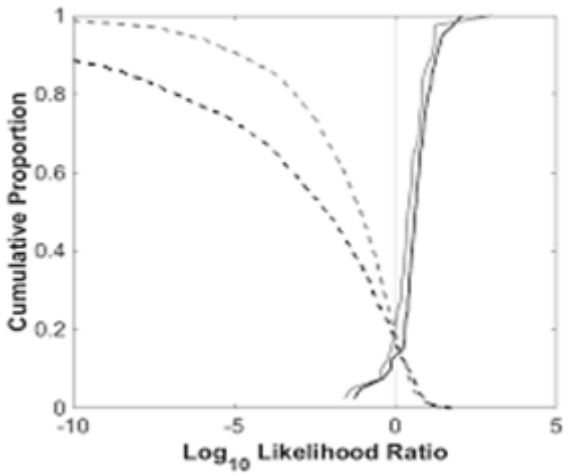

Fig 8: Cumulative evidence batch proportion

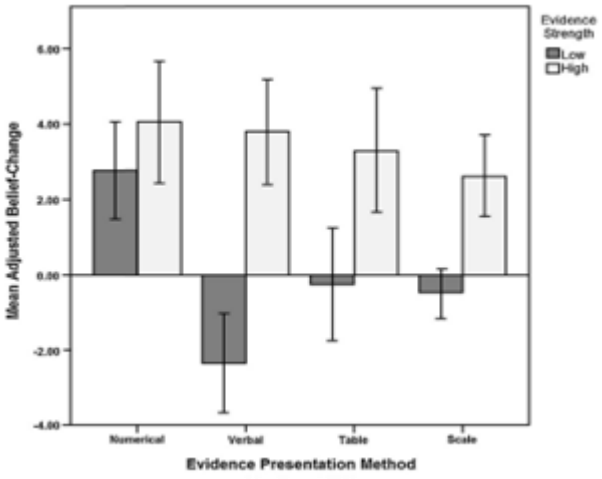

Fig 9: Depicts the strength of the evidence batch

Batch proportion for each evidence group has made the cumulative results and it depicts the highest value range molded with most likelihood ratio and moving upwards which shows the evidence strength normalization and has the look around value probably falling under the range of -10 to 5 and the digital parameters considers to be directly proportional once it reaches to the threshold value. Every batch has its own weakness and strength which highly

supports the digital parameters to be monitored in order to arrange the most likelihood values. The batch strength [2][11[13] depicted in the framework realizes the co efficient values may deviate drastically once the digital crime scene time period goes on. It represented two categorical values range as low and high and every batch evaluation process, the numerical labels and verbal labels are considered. This gave the maximum likelihood values where the strength of the categorical labels might be degraded according to the time frame.

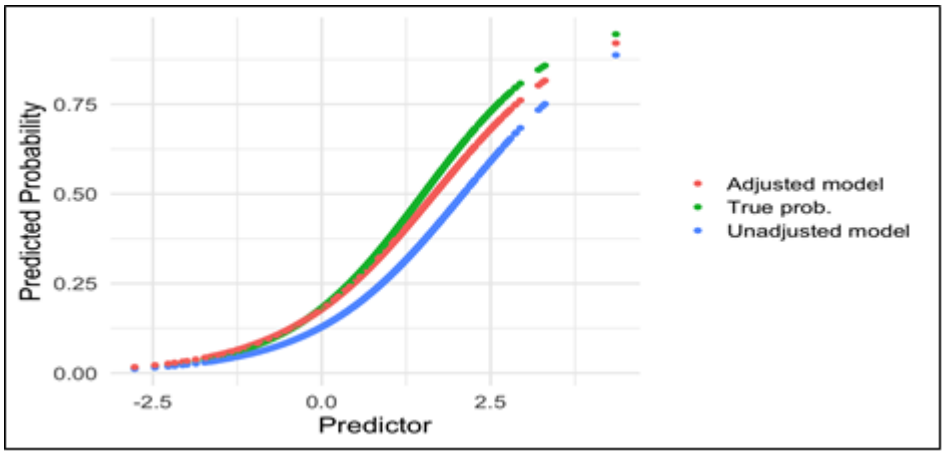

Fig 10: Kernel density evaluation with Likelihood procedure

The framework is able to handle the KDE based evaluation model and the histogram represented the ratio of certain evidence batch with its corresponding labelling range. LR is modeled by the limit of positive and negative tolerance and the prediction labelled as per the probability values. The system considers the predictor probability in the range of 0 to 0.75 and the prediction made on the range of -2.5 to 2.5. These ranges calculate the true probability mode which deviates to the adjusted and unadjusted labelling range according the strength of the evidence.

6. Conclusion

A new framework developed with stable evaluation modules for handling digital forensic evidences under handheld devices. Most of the handheld devices forensic tools manages the evidence priority and its time frame calculation and omits the evidences which are less parameterized consideration. The tools can handle the evidence files as bunch where a limited characterized patters are coded and may fail during the dynamic evaluation of sensitive evidences. This problem occurs in most of the tools which are applicable for digital forensics. Here the framework showed a new categorical and time bound mechanism where dynamic case studies and evaluations can be uploaded during the evaluation time. The system works based on the standard evidence processing mechanism where the collection of evidences are crucial and critical as time goes on. Numerical and Verbal based Likelihood ratio and its processing done on the calculation module also it categorized certain evidence file to be processed according to the standard module structure. KDE and likelihood procedure used in this framework is capable of handling many of the sensitive digital evidences and it produced a certain satiasfiable level of accuracy. Manual and logical level evidence extraction is the additional parametric used in the framework and every modules implies a certain number of evaluation criteria which should be passed to proceed with the next level of evaluation. It combines evidence bunch and history pouch with sensitive criteria and may load digital scene report as an additional file for the categorical labels. The likelihood ratio and it comparison on the evidence bunch may proceed with the report and it combines micro content and uncertainty data at the same time. 8 characteristics evaluation are applied to the modules and the processed evidences are stored with additional tool integration if needed. The framework can be served as the best analytical and prediction tool for digital forensics.

References

[1] Martire, K. A., Kemp, R. I., Sayle, M., & Newell, B. R. (2014). On the interpretation of likelihood ratios in forensic science evidence: Presentation formats and the weak evidence effect. Forensic Science International, 240, 61–68. http://dx.doi.org/10.1016/j.forsciint.2014.04.005

[2] Bolck A and Alberink I (2011), Variation in Likelihood Ratios for forensic evidence evaluation of XTC tablets comparison, Journal of Chemometrics , 25: 41-49 DOI: 10.1002/cem.1361.

[3] Martire, K. A., Kemp, R. I., Watkins, I., Sayle, M. A., & Newell, B. R. (2013). The expression and interpretation of uncertain forensic science evidence: Verbal equivalence, evidence strength, and the weak evidence effect. Law and Human Behavior, 37, 197–207. http://dx.doi.org/ 10.1037/lhb0000027.

[4] Neumann C, Champod C, Puch-Solis R, Egli N, Anthonioz A, Bromage-Griffiths A, (2007), Computation of Likelihood Ratios in Fingerprint

Identification for Configurations of Any Number of Minutiae, J Forensic Sci, 54-64.

[5] Weyermann C, Marquis R, Delaporte C, Esseiva P, Dujourdy L, Lock E, Aalberg L, Dieckmann S, Zrcek F, Bosenko J (2008), Drug intelligence based on MDMA tablets data: (1) Organic impurities profiling. Forensic Science International 177 (1):11-16.

[6] Marquis R, Weyermann C, Delaporte C, Esseiva P, Dujourdy L, Koper C, Aalberg L, Dahlenburg R, Zrcek F, Bosenko J (2008) Drug intelligence based on MDMA tablets data: (2) Phusical characteristics profiling. Forensic Science International 178 (1): 24-39.

[7] Bayes T, Price, R (1763). An Essay towards solving a Problem in the Doctrine of Chance. By the late Rev. Mr. Bayes, communicated by Mr. Price, in a letter to John Canton, M. A. and F. R. S. Philosophical Transactions of the Royal Society of London 53: 370–418.

[8] Cole, S. Forensics Without Uniqueness, Conclusions Without Individualization: The New Epistemology of Forensic Identification. Law, Probability and Risk 2009, 8 (3), 233–255

[9] Koehler, J. J., & Macchi, L. (2004). Thinking about low-probability events. An Exemplar-Cuing theory. Psychological Science, 15, 540–546. http:// dx.doi.org/10.1111/j.0956-7976.2004. 00716.x

[10] Evett, I. W.; Lambert, J. A.; Buckleton, J. S. A Bayesian Approach to Interpreting Footwear Marks in Forensic Casework. Sci. and Justice 1998, 38 (4), 241–247.

[11] Thomson, W. C. Discussion Paper: Hard Cases Make Bad Law–Reactions to R v T. Law, Probability and Risk 2012, 11 (4), 347–359.

[12] Ponce, A., and F. Pascual. 1999. Critical review of presumptive tests for bloodstains. Forensic Science Communications 1(2). http://www.fbi.gov/about-us/lab/forensic-sciencecommunications/ fsc/archive/july1999/ponce.htm (accessed March 10, 2011).

[13] Adderley, R., Bond, J.W., Townsley, M. Use of data mining techniques to model crime scene investigator performance 26th SGAI International Conference on Innovative Techniques and Applications of Artificial Intelligence, Cambridge UK, 2006.

[14] Skopik, Settanni, & Fiedler (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154–176. doi.org/10.1016/j.cose.2016.04.003.

[15] Harris, A. Corner, U. Hahn, James is polite and punctual (and useless): a Bayesian formalisation of faint praise, THINK REASONING (2013), http:// dx.doi.org/10.1080/13546783.2013.801367.

[16] Taroni, F., Aitken, C., Garbolino, P., & Biedermann, A. (2006). Bayesian networks and probabilistic inference in forensic science. West Sussex, UK: Wiley. http://dx.doi.org/10.1002/0470091754

[17] Christensen, Michael E. RaynorRory McDonald (2015). What Is Disruptive Innovation? Harvard Business Review, 44–53. Retrieved from https://hbr.org/2015/12/what-is-disruptive-innovation.

[18] Taroni, F., Aitken, C., Garbolino, P., & Biedermann, A. (2006). Bayesian networks and probabilistic inference in forensic science. West Sussex, UK: Wiley. http://dx.doi.org/10.1002/0470091754

[19] Tversky, A., & Kahneman, D. (1982). Evidential impact of base rates. In D. Kahneman, P. Slovic, & A. Tversky (Eds.), Judgment under uncertainty: Heuristics and biases (pp. 153–160). Cambridge, UK: Cambridge University Press. http://dx.doi.org/10.1017/CBO9780511809477.011

[20] Thompson, W. C., Kaasa, S. O., & Peterson, T. (2013). Do jurors give appropriate weight to forensic identification evidence? Journal of Empirical Legal Studies, 10, 359–397. http://dx.doi.org/10.1111/jels.12013

[21] Thompson, W. C. (2012). Discussion paper: Hard cases make bad law: Reactions to R v. T. Law Probability and Risk, 11, 347–359. http://dx .doi.org/10.1093/lpr/mgs020

[22] Cankaya EC, Kupka B. A Survey of Digital Forensics Tools for Database Extraction. In Future Technologies Conference; 2016; San Fransisco: IEEE. p. 1014-1019.

[23] [J. Beckett and J. Slay, “Digital forensics: Validation and verification in a dynamic work environment,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., no. February 2014, 2007.

[24] Riadi and A. Firdonsyah, “Forensic Investigation Technique on Android ’ s Blackberry Messenger using NIST Framework,” Int. J. Cyber - Secur. Digit. Forensics (IJCSDF) Soc. Digit. Inf. Wirel. Commun., vol. 6, no. 4, pp. 198–205.