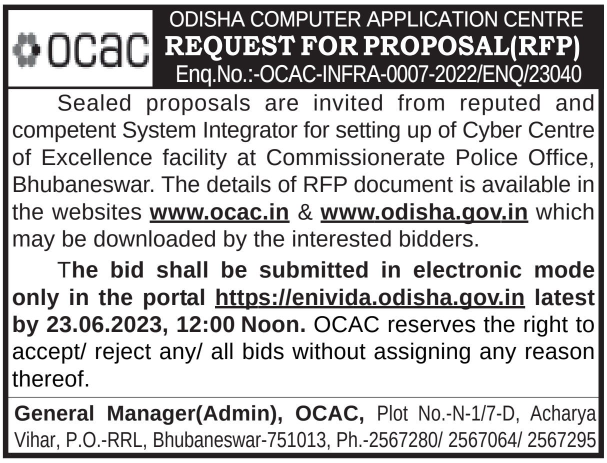

ODISHA COMPUTER APPLICATION CENTRE

REQUEST FOR PROPOSAL(RFP)

Enq.No.:-OCAC-INFRA-0007-2022/ENQ/23040

Sealed proposals are invited from reputed and competent System Integrator for setting up of Cyber Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar. The details of RFP document is available in the websites **www.ocac.in** & **www.odisha.gov.in** which may be downloaded by the interested bidders.

T**he bid shall be submitted in electronic mode only in the portal https://enivida.odisha.gov.in latest by 23.06.2023, 12:00 Noon.** OCAC reserves the right to accept/ reject any/ all bids without assigning any reason thereof.

General Manager(Admin), OCAC, Plot No.-N-1/7-D, Acharya Vihar, P.O.-RRL, Bhubaneswar-751013, Ph.-2567280/ 2567064/ 2567295

Request for Proposal

RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Government of Odisha

RFP Ref. No.: -OCAC-SEGP-INFRA-0007-2022-23040

ODISHA COMPUTER APPLICATION CENTRE
[TECHNICAL DIRECTORATE OF E&IT DEPARTMENT, GOVERNMENT OF ODISHA]
OCAC Building, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India
W: www.ocac.in | **T**: 0674-2567295/2567283 | **F**: 0674-2567842

Table of Contents

1 GLOSSARY OF TERMS

BG	Bank Guarantee
BCP	Business Continuity Plan
CP Office	Commissionerate Police office
E&IT	Electronics and Information Technology
EMD	Earnest Money Deposit
e-Nivida	e-Procurement Platform Solution
ICT	Information and Communication Technology
ITES	Information Technology Enabled Services
L1 Bidder	Bidder with L1(Lowest) Quote
L1 quote	Lowest price discovered through Commercial Bid
QCBS	Quality And Cost Based Selection
OCAC	Odisha Computer Application Centre
PBG	Performance Bank Guarantee
RFP	Request For Proposal
SDC	State Data Centre
SI	System Integrator
SP	Service Provider/Solution Provider
TOR	Terms of Reference

2 FACT SHEET

Sl#	Item	Description
a)	Project Title	RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha
b)	Name of Purchaser	Odisha Computer Application Centre
c)	Contact Person, Address and Email	General Manager (Admin) Plot No. N-1/7-D, Acharya Vihar RRL Post Office, Bhubaneswar Odisha - 751013 gm_ocac@ocac.in
d)	RFP Document Fees	₹11,200/- inclusive of GST @ 12% (Rupees Eleven Thousand and Two Hundred only)
e)	Earnest Money Deposit	₹1,00,00,000/- (rupees One Crore only) in shape of DD/RTGS or BG
f)	Selection Method	QUALITY AND COST BASED SELECTION (QCBS)-(70% Weightage on Technical and 30% Weightage on Commercial Evaluation)
g)	Last date for submission of queries by Bidders	**By 4 PM of 07-06-2023**
h)	Pre-bid Meeting	**09-06-2023 at 12 Noon (in VC mode)**
i)	Last date and time for receipt of proposals from Bidders	**23-06-2023 by 12 Noon through e-Nivide Portal (www.enivida.odisha.gov.in)**
j)	Date and time for opening of Prequalification bid & Technical bid	**23-06-2023 by 3:30 PM**
k)	Date and time for Technical Presentation	To be notified later
l)	Date and time for opening of Commercial Bids	To be notified later
m)	Bid Validity Period	180 Days from date of submission of bid
n)	Project Term	Contract duration would be 64 months from the date of work order

3 REQUEST FOR PROPOSAL

Sealed proposals are invited from eligible, reputed, qualified System Integrator for provision of Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha and manage the same for a period of 5 years from the date of commissioning of service. The details of scope of work are mentioned in the **Terms of Reference** section of this Request for Proposal (RFP) Document. This invitation to bid is open to all bidders meeting the minimum eligibility criteria as mentioned in this RFP Document.

4 STRUCTURE OF THE RFP

This RFP document for "RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha" comprises of the following.

a) Instructions on the Bid process for the purpose of responding to this RFP. This broadly covers:
   i) General instructions for bidding process
   ii) Bid evaluation process including the parameters for Pre-qualification, Technical Evaluation and Commercial Evaluation for determining bidder's suitability as the system integrator
   iii) Commercial bid and other formats

b) Functional and Technical Requirements of the project. The contents of the document broadly cover the following areas:
   i) About the project and its objectives
   ii) Scope of work
   iii) Timeline
   iv) Service levels

The bidder is expected to respond to the requirements as completely and in as much relevant detail as possible and focus on demonstrating bidder's suitability to become the System Integrator of OCAC for this assignment.

The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the bidder's risk and may result in the rejection of the proposal.

5 BACKGROUND INFORMATION

5.1 Basic Information

OCAC, the technical directorate of E & IT Department, Government of Odisha invites responses ("Tenders") to this Request for Proposals ("RFP") from System Integrators for ("Bidders") Selection of SI to set up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha as described in this RFP, "Terms of Reference".

Proposals must be received not later than time, date and venue mentioned in the Fact Sheet. Proposals that are received late will not be considered in this procurement process.

OCAC will award the Contract to the successful bidder whose proposal has been determined as the best value proposal based on Technical and Financial evaluation criteria and accepted by the Authority.

5.2 Project Background

Cybercrime is becoming a global phenomenon and a worldwide concern. As cybercriminals face no boundaries, the traditional law enforcement approach is becoming superseded. A vital aspect to fight against cybercrime is that, the State Law Enforcement Agency is to have Centre of Excellence for Cyber Security. Also, to establish cyber intelligence, investigation and forensic units those are fully prepared both from the equipment and the knowledge point of view to face cybercriminals and their destructive actions.

As an initiative, Odisha Computer Application Centre (OCAC) and Government of Odisha is intended to setup Centre of Excellence (CoE) for Cyber Security enabled with tools, technologies, process, and trained manpower to combat the Cybercriminals. The COE will be the nodal point of contact and advisory agency for the State in cybercrime investigation and enablement.

To efficiently handle the cybercrime investigations and analytics, it is pertinent to have skilled manpower in these core areas. One of the important aspects of this project is to have an effective cyber security workforce.

The key objectives and functional requirement of the Centre of Excellence are -

- To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.
- Planning, designing, and analyzing cyber security capacity building program for the Government of Odisha (GoO).
- To organize Awareness, Training and Education program, as depicted in (but not limited to) the standards like National Institute of Standards and Technology (NIST) Special Publication 800-50, Advisories from NCIIPC and CERT-In.

- To create awareness, train and educate the citizens of Odisha, Police officials of cybercrime department and create a cybersecurity workforce with necessary capacity and capability for cyber resilience.
- To develop necessary workforce within government and law enforcement agencies/public prosecutors, pleaders/judicial officials in digital forensics and technology assisted investigation techniques.
- To develop tools, technologies, Standard Operating Procedures (SOPs) and establish Best Practices.
- To study and develop policies and advisories regarding various domains of Cyber Security and its allied domains, etc.
- To create and facilitate various services regarding Cyber Security and its allied domains.

5.3 Broad Scope of work

The section provides a broad level of scope of services for the understanding of the bidders.

1. The primary scope of this RFP is to procure necessary Cyber forensic tools for the Department to carry out investigation, monitoring, data, evidence analytics and prosecution.
2. The Successful Bidder shall ensure implementation of the proposed cyber forensic tools as per the scope defined in the RFP.
3. The proposed forensics tools, social media Tools and Crime data analytics, equipment's shall provide technical aid in investigation and prosecution and speed up the investigation process.
4. The successful bidder shall need to provide their solutions under these Five major components.

    I. Cyber Forensic Tools

    II. Cyber Forensic Tools Training to the officers

    III. Provide manpower to operate the center.

    IV. Assist in Cybercrime investigation

    V. Simulation Lab to test & validate Malicious Code/Software.

Note: OCAC / Odisha Police Department shall provide necessary underlying physical & logical infrastructure & facilities required to successfully set up and operate Cyber Forensic hardware and software.

6 INSTRUCTION TO THE BIDDERS

6.1 General

a) While efforts have been made to provide comprehensive and accurate background information, requirements and specifications, Bidders must form their own conclusions about the solution needed to meet requirements. Also, bidders may wish to consult their own legal advisers in relation to this RFP.

b) All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the assignment by OCAC on the basis of this RFP.

c) No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of OCAC. Any notification of preferred Bidder status by OCAC shall not give rise to any enforceable rights by the Bidder. OCAC may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of OCAC.

d) This RFP supersedes and replaces any previous public documentation and communications, and Bidders should place no reliance and dependence on such communications.

6.2 Compliant Proposals / Completeness of Response

a) Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

b) Failure to comply with the requirements of this paragraph may render the Proposal non-compliant and the Proposal may be rejected. Bidders must:

   - Include all documentation specified in this RFP.
   - Follow the format of this RFP and respond to each element in the order as set out in this RFP.
   - Comply with all requirements as set out within this RFP.

6.3 Code of integrity

No official of a procuring entity or a bidder shall act in contravention of the codes which includes

a. prohibition of

   i. Making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process.

   ii. Any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained or an obligation avoided.

   iii. Any collusion, bid rigging or anticompetitive behavior that may impair the transparency, fairness and the progress of the procurement process.

   iv. Improper use of information provided by the procuring entity to the bidder with an intent to gain unfair advantage in the procurement process or for personal gain.

   v. Any financial or business transactions between the bidder and any official of the procuring entity related to tender or execution process of contract; which can affect the decision of the procuring entity directly or indirectly.

   vi. Any coercion or any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process.

vii. Obstruction of any investigation or auditing of a procurement process.

viii. Making false declaration or providing false information for participation in a tender process or to secure a contract;

b. Disclosure of conflict of interest.

c. Disclosure by the bidder of any previous transgressions made in respect of the provisions of sub-clause (a) with any entity in any country during the last three years or of being debarred by any other procuring entity.

d. In case of any reported violations, the procuring entity, after giving a reasonable opportunity of being heard, comes to the conclusion that a bidder or prospective bidder, as the case may be, has contravened the code of integrity, may take appropriate measures.

6.4 Pre-Bid Meeting and Clarifications

6.4.1 Pre-Bid conference

a) OCAC shall hold a pre-bid meeting with the prospective bidders on **the date mentioned in the fact sheet in VC Mode** (through Microsoft Teams).

b) Link will be provided to the interested bidders on request through email to gm_ocac@ocac.in (with a copy to tushar.mohapatra@ocac.in) before the meeting starts through their e-mail-ID**.**

c) The representatives of Bidders (restricted to two persons) may attend the Pre-bid meeting.

d) The Bidders should submit their queries in writing in below specified format (in MS-Excel only) by the schedule as mentioned in this RFP, prior to attending the pre-bid meeting. **Any other format shall not be entertained**

Sl#	RFP Document Reference(s) (Section & Page Number(s))	Content of RFP requiring Clarification(s)	Points of Clarification

e) OCAC shall not be responsible for any Bidders' queries received by it in any other format. Any requests for clarifications post the indicated date and time mentioned will not be entertained by OCAC.

6.4.2 Responses to Pre-Bid Queries and Issue of Corrigendum

a) The Nodal officer notified by OCAC will provide timely response to all queries. However, OCAC neither makes representation or warranty as to the completeness or accuracy of any response made in good faith, nor does OCAC undertake to answer all the queries that have been posed by the Bidders.

b) At any time prior to the last date for receipt of bids, OCAC may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP document by corrigenda and/or addenda.

c) The Corrigendum (if any) and clarifications to the queries from all Bidders will be posted on www.enivida.odisha.gov.in , www.ocac.in or www.odisha.gov.in

d) Any such corrigenda and/or addenda shall be deemed to be part of this RFP.

e) In order to provide prospective Bidders reasonable time for taking the corrigenda and/or addenda into account, OCAC may, at its discretion, extend the last date for the receipt of Proposals

6.5 Key Requirements of the Bid

6.5.1 Right to Terminate the Process

a) OCAC may terminate the RFP process at any time and without assigning any reason. OCAC makes no commitments, express or implied, that this process will result in a business transaction with anyone.

b) This RFP does not constitute an offer by OCAC. The Bidder's participation in this process may result in OCAC selecting the Bidder to engage towards execution of the contract.

6.5.2 RFP Document Fees

The bidder must furnish along with its bid required bid document fee amounting to ₹11,200/- inclusive of GST @ 12% online through e-Nivida portal/or in shape of DD in favor of “Odisha Computer Application Centre” payable at Bhubaneswar.

The fee can also be paid through electronic mode to the following:

Bank A/c No. : 149311100000195
Payee Name : Odisha Computer Application Center
Bank Name & Branch : Union Bank of Inidia, Acharya Vihar, Bhubaneswar
Account Type: Savings
IFSC : UBIN0814938

6.5.3 Earnest Money Deposit

a) Bidders shall submit, along with their Bids, EMD of **₹1,00,00,000/-** (One Crore) in the shape of Bank Draft **OR** Bank Guarantee (in the format specified in this RFP at Clause no. 10.1.7) issued by any scheduled bank in favour of Odisha Computer Application Centre, payable at Bhubaneswar, and should be valid for 180 days from the due date of the tender / RFP. The EMD should be submitted in the General Bid.

b) The EMD may also paid through electronic mode to the following financial

Bank A/c No. : 149311100000195
Payee Name : Odisha Computer Application Center
Bank Name & Branch : Union Bank of Inidia, Acharya Vihar, Bhubaneswar
Account Type: Savings

IFSC : UBIN0814938

c) EMD of all unsuccessful bidders would be refunded by OCAC within 60 days of the bidder being notified as being unsuccessful. The EMD, for the amount mentioned above, of successful bidder would be returned upon submission of Performance Bank Guarantee.

d) The EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.

e) The bid / proposal submitted without EMD, mentioned above, will be summarily rejected.

f) The EMD may be forfeited:

   i) If a bidder withdraws its bid during the period of bid validity.

   ii) In case of a successful bidder, if the bidder fails to sign the contract in accordance with this RFP.

   iii) If found to have a record of poor performance such as having abandoned work, having been black-listed, having inordinately delayed completion and having faced Commercial failures etc.

   iv) The Bidder being found to have indulged in any suppression of facts, furnishing of fraudulent statement, misconduct, or other dishonest or other ethically improper activity, in relation to this RFP

   v) A Proposal contains deviations (except when provided in conformity with the RFP) conditional offers and partial offers.

6.6 Submission of proposal

6.6.1 Instruction to Bidders for Online Bid Submission

e-Nivida is a complete process of e-Tendering, from publishing of tenders online, inviting online bids, evaluation and award of contract using the system. The instructions given below are meant to assist the bidders in registering on e-Nivida Portal and submitting their bid online on the portal.

More information useful for submitting online bids on the e-Nivida Portal may be obtained at: https://enivida.odisha.gov.in

6.6.2 Guidelines for Registration

a) Bidders are required to enroll themselves on the eNivida Portal https://enivida.odisha.gov.in or click on the link “Bidder Enrolment” available on the home page by paying Registration Fees of Rs.2,800/- + Applicable GST.

b) As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.

c) Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication with the bidders.

d) Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Only Class III Certificates with signing + encryption key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify/ TCS / nCode/ eMudhra etc.), with their profile.

e) Only valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.

f) Bidder then logs in to the site through the secured log-in by entering their user ID /password and the password of the DSC / e-Token.

g) The scanned copies of all original documents should be uploaded in pdf format on e-tender portal.

h) After completion of registration payment, bidders need to send their acknowledgement copy on our help desk mail id odishaenivida@gmail.com for activation of the account.

6.6.3 Searching for Tender Documents

a) There are various search options built in the e-tender Portal, to facilitate bidders to search active tenders by several parameters.

b) Once the bidders have selected the tenders they are interested in, then they can pay the Tender fee and processing fee (NOT REFUNDABLE) by net-banking / Debit / Credit card then you may download the required documents / tender schedules, Bid documents etc. Once you pay both fee tenders will be moved to the respective 'requested' Tab. This would enable the e- tender Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.

6.6.4 Preparation of Bids

a) Bidder should take into account any corrigendum published on the tender document before submitting their bids.

b) Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.

c) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF formats. Bid Original documents may be scanned with 100 dpi with Colour option which helps in reducing size of the scanned document.
To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, GST, Annual reports,

auditor certificates etc.) has been provided to the bidders. Bidders can use “My Documents” available to them to upload such documents.

d) These documents may be directly submitted from the “My Documents” area while submitting a bid and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process. Already uploaded documents in this section will be displayed. Click “New” to upload new documents.

6.6.5 Submission of Bids

a) Bidder should log into the website well in advance for the submission of the bid so that it gets uploaded well in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.

b) The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document as a token of acceptance of the terms and conditions laid down by Department.

c) Bidder has to select the payment option as per the tender document to pay the tender fee / Tender Processing fee & EMD as applicable and enter details of the instrument.

d) In case of BG bidder should prepare the BG as per the instructions specified in the tender document. The BG in original should be posted/couriered/given in person to the concerned official before the Online Opening of Financial Bid. In case of non-receipt of BG amount in original by the said time, the uploaded bid will be summarily rejected.

e) Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOQ format with the tender document, then the same isto be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete the yellow coloured (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If theBOQ file is found to be modified by the bidder, the bid will be rejected.

f) The server time (which is displayed on the bidders’ dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.

g) The uploaded bid documents become readable only after the tender opening by the authorized bid openers.

h) Upon the successful and timely submission of bid click “Complete” (i.e. after clicking “Submit” in the portal), the portal will give a successful Tender submission acknowledgement & a bid summary will be displayed with the unique id and date & time of submission of the bid with all other relevant details.

i) The tender summary has to be printed and kept as an acknowledgement of the submission of the tender. This acknowledgement may be used as an entry pass for any bid opening meetings.

6.6.6 Clarifications on using e-Nivida Portal

a) Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.

b) Any queries relating to the process of online bid submission or queries relating to e-tender Portal in general may be directed to the Helpdesk Support.

Please feel free to contact e-Nivida Helpdesk (as given below) for any query related to e-tendering.

Phone No.: 011-49606060
Email id: odishaenivida@gmail.com
www.enivida.odisha.gov.in

6.6.7 Tender Validity

Proposals shall remain valid for a period of 180 Days from the date of opening of the pre-qualification and technical proposals. OCAC reserves the rights to reject a proposal valid for a shorter period as non- responsive and will make the best efforts to finalize the selection process and award of the contract within the bid validity period. The bid validity period may be extended on mutual consent.

6.6.8 Submission and Opening of Proposals (electronic mode only)

a) The bidders should submit their responses as per format given in this RFP in the following manner:

- Response to Pre-Qualification Criterion
- Technical Proposal
- Commercial Proposal

b) Please Note that Prices should not be indicated in the Pre-Qualification Response or Technical Proposal but should only be indicated in the Commercial Proposal.

c) The Response to Pre-Qualification criterion, Technical Proposal and Commercial Proposal (as mentioned in previous paragraph) should be submitted through online mode in e-Nivida Portal.

d) The Proposals submitted in time as per fact sheet will be opened as per the schedule mentioned in the fact sheet

6.6.9 Bids in other form

a) The bids submitted in hard copy or by post/e-mail etc. **shall not be considered** and no correspondence will be entertained on this matter.

b) OCAC reserves the right to modify and amend any of the above-stipulated condition/criterion depending upon project priorities vis-à-vis urgent commitments.

6.6.10 Proposal Preparation Costs

The bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings or discussions or presentations, preparation of Proposal, in providing any additional information required by OCAC to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process.

OCAC will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

6.6.11 Language

The Proposal should be filled by the Bidder in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by Bidders. For purposes of interpretation of the Proposal, English translation shall govern.

6.6.12 Acceptance and Rejection of Bids

OCAC reserves the right to reject in full or part, any or all bids without assigning any reason thereof. OCAC reserves the right to assess the Bidder’s capability and capacity. The decision of OCAC shall be final and binding. Bid should be free of overwriting. All measures, correction or addition must be clearly written both in words and figures and attested. Offers not submitted in prescribed manner or submitted after due date and time are liable to rejection.

6.7 Evaluation Process

a) OCAC/ Police Commissionerate Office will constitute a Proposal Evaluation Committee to evaluate the responses of the bidders.

b) The Proposal Evaluation Committee constituted by OCAC/ Police

Commissionerate Office shall evaluate the

Responses to RFP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence, may lead to rejection of the bid.

c) The decision of Proposal Evaluation Committee in evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of negotiation/ discussion with the Committee.

d) The Proposal Evaluation Committee may ask for meetings with the Bidders to seek clarifications on their proposals, if required.

e) The Proposal Evaluation Committee reserves the right to reject any or all proposals on the basis of any deviations.

f) Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.

g) Initial bid scrutiny will be held, and incomplete details as given below will be treated as nonresponsive if proposals are:

- Not submitted as specified in the RFP document
- Received without the Letter of Authorization (Power of Attorney)
- Found with suppression of details
- Found with incomplete information, subjective, conditional offers and partial offers submitted
- Submitted without the documents requested in checklist
- Submitted with lesser validity period

h) All responsive Bids will be considered for further processing as below:

OCAC will prepare a list of responsive bidders, who comply with all the Terms and Conditions of RFP. All eligible bids will be considered for further evaluation by a Committee according to the evaluation process defined in this RFP document. The decision of the Committee will be final in this regard.

7 CRITERIA FOR EVALUATION

The overall objective of this evaluation process is to select the capable and qualified firm and providing associated capacity building, training and operations & maintenance support.

The Pre-Qualification proposal will be evaluated as per criteria mentioned below and only those bidders who qualify the requirements will be eligible for next set of evaluations. Technical Proposal and Commercial Proposal of Bidders who do not meet the Pre-Qualification criteria will not be opened in the portal

The technical score of all the bidders would be calculated as per the criteria mentioned below. All the bidders who achieve more than 70 marks in the technical evaluation would be eligible for the next stage, i.e. Commercial Bid opening.

Bidders should submit supporting documentary evidence with respect to the above, in absence of which their proposals will be summarily rejected.

7.1 Pre-Qualification Criteria (Level-1 Evaluation)

Sl#	Basic Requirement	Specific Requirement	Documents required
1.	Legal Entity	The bidder must be a company registered in India under Indian Companies Act 1956/2013 OR A Partnership firm registered under Indian Partnership Act, 1932, The bidder must be in operation in India since last 5 years as on 31st December 2022. The bidder must have GST registration & up-to-date Income Tax Return, Valid PAN Number as on 31st March 2022.	a. Valid copy of certificate of incorporation and registration certificates. b. Copy of GST registration. c. Copies of relevant Certificates of registrationIncome Tax / PAN
2.	Turnover	The bidder's turnover in the field of Cyber Security/ Surveillance/Forensics/Smart City should be minimum of 50 crores in last three financial years.	Balance Sheet/CA Certificate
		The bidder should have minimum 1 completed/Ongoing projects having Integrated Command and Control as a component.	LoI/Work order indicating ICC as component.
3.	Net Worth	The net worth of the bidder should be positive for the last 3 financial years	- CA Certificate

4.	OEM Experiences	The Bidder/OEM {themselves or through reseller(s)} should have regularly, manufactured and supplied same or similar Products to any Central / State Govt Organization / PSU / Global/Public Listed Company.	Copies of relevant documents to be submitted along with bid.
5	Bidder Technical -Capability	The Bidder must have undertaken at least 1 project pertaining to Forensics / Cyber Security / Network Security in Central / State Govt Organization / PSU/Public Listed Company. with a minimum project value of Rs. 8 crores in the last 5 years, as on the date of submission of this RFP.	Copy of original PO/CA Certificate
6	Bidder Working capital	The working capital of the bidder shall be more than Rs. 50 Cr	CA Certificate
7	Bidder Experience	Bidders should have min 5 years of experience in providing Cyber Security/Forensics services.	PO Copy/Self Declaration
8	Bidder Experience	Bidder should have his or her own ISO 27001 certified operational Managed Security Operations Centre (SOC) in India.	Certification Required
9	Bidder Experience	The Bidder must have at least 100 IT/computer professionals, out of which minimum ten (10) professionals having any of the certifications like CISA/ CISM/ CEH/ CHFI/ GCIH/ CISSP/ CEH/ OSCP/ ISO 27001/ CISSP/ GCFA/ master's in cyber/Digital forensics working continuously full time for the past 1 year at the time of submission of bids.	Certificate from the HR head regarding the same.

10	Quality Certification	The bidder must possess a valid ISO 9001, & ISO27001 Certification.	Copies of the validcertificates.
11	Blacklisting	The bidder should not be under a declaration of ineligibility for corrupt and fraudulent practices issued by any Government in India. The bidder should not be Blacklisted by any Govt/PSU/BFSI/Telecom/ISP	Self-declaration
12	OEM Authorization	The bidder must attach Manufactures Authorization certificate specific to this tender & Back-to-back support letters from OEMs for providing Comprehensive support and services of the OEM's product covered under the RFP. MAF should contain the details of authorized signatory which includes Full name, designation, mobile no., email id) and should be digitally signed.	OEM MAF
13	Local Presence	The bidder should have an office in Odisha. However, if the presence is not there in the state, the bidder should give an undertaking for the establishment of an office, within one month of the award of the contract.	Relevant Documents supporting office addresses/ Undertaking.
14	DocumentFee	The bidder must have made a payment of ₹11,200.00 (Rupees Eleven Thousand Two Hundred Only) (Inclusive of GST) towards tender document fee.	Online at e-Nivida Portal
15	EMD	INR 1,00,00,000/- (One Crore)	in shape of DD or BG

7.2 **Technical Evaluation** Level-2 Evaluation)

7.2.1 Bidder must quote all the products/equipment mentioned in the Bill of

Materials. Otherwise, the bid will not be considered.

7.2.2 Bidder must furnish tender-specific Manufacture Authorization Form against the entire item mentioned in the Bill of Material.

7.2.3 Bidder must furnish the unpriced bill of materials of the items quoted in the technical bid.

7.2.4 Bidder should accept the entire scope of work (including services) as mentioned in the Scope of work.

7.2.5 The Bidder/OEM must have experience with the Proposed requirements and should be implemented and running in Public/Government entity in India. (The bidder may submit Copy of original PO, Contract Completion Certificate or Installation Report or Credential letter from client working specifying project completion).

7.2.6 The Product offered should meet all the technical and functional requirements given in the "Specification Section"

7.2.7 All the compliances should be submitted on OEM Letterhead.

7.2.8 The bidder should furnish documentation in technical bid and make demonstration/presentation on the proposed solution as per following parameters before bid evaluation committee. Based on the documentation and presentation/demonstration mark shall be awarded.

Technical Evaluation Scoring Matrix

Sl#	Evaluation Criterion	Maximum Marks	Documents Required
2	Bidder should have experience in Cyber Security Projects. Each project 5 marks	15	Work order
3	Bidder should have experience in smart city / Surveillance / ICCC. Each project 5 marks	15	Work order
4	The Bidder shall own Forensic Lab / SOC that provides services in India in last 5 years Each Project 10 Marks	20	Self Declaration
5	Presentation	50	
6	The Bidder shall have Experience in Supplying and commissioning same Malware Testing Lab Software Solution bided in this RFP (Digital Twin/Range) to at least one government regulators/CERT	15	Work Order and completion

a) The bidder must comply to the specification of the items.

b) All the bidders who secure a Technical Score of 70% or more will be declared as technically qualified.

c) The bidder with highest technical bid (H1) will be awarded 100% score.

d) Technical Score of a Bidder(Tn) = {(Technical Bid Score of the Bidder / Technical Bid Score of H1) X 100} %

(Adjusted up to two decimal places)

e) The commercial bids of only the technically qualified bidders will be opened for further processing.

7.3 Financial Bids Evaluation Level-3 Evaluation)

a) Bidders will be selected through QCBS - Quality & Cost Based Selection with Technical and Financial ratio of 70:30.

b) The Financial Bids of the technically qualified bidders (those have secured more than 70% of mark in technical evaluation) will be opened on the prescribed date in the presence of bidders' representatives.

c) Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.

d) The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.

e) Any conditional bid would be rejected.

f) Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail. If the bidder does not accept the correction of error, its bid will be rejected”.

g) If there is no price quoted for certain material or service, the bid shall be declared as disqualified.

h) In the event that there are 2 or more bidders having the same value in commercial bid, the bidder securing highest technical score will be adjudicated as “Best responsive bid” for award of the Project.

i) The bidder with lowest qualifying financial bid (L1) will be awarded 100% score. Financial score for other bidders will be evaluated using the following formula;
Financial Score of a Bidder(Fn)={(Financial Bid of L1/ Financial Bid of the Bidder) X 100} %

(Adjusted up to two decimal Places)

7.4 Final Evaluation of Bids (Final Evaluation)

The technical and financial evaluation scores secured by each bidder will be added using weightages of 70% and 30% respectively to compute composite score.

The formula for the calculation of the Composite score

Bn = 0.70 * Tn + 0.30* Fn

Where:

Bn = overall score of bidder

Tn = Technical score of the bidder (out of maximum of 100 marks)

Fn = Normalized financial score of the bidder

The Bidder securing Highest Composite Bid Score will be adjudicated with the Best Value Bidder for award of the project.

8 APPOINTMENT OF SYSTEM INTEGRATOR

8.1 Award Criteria

Purchaser will award the Contract to the successful Bidder whose proposal determined to be substantially responsive and has been determined as the most responsive bids as per the process outlined above.

8.2 Right to Accept Any Proposal and To Reject Any or All Proposal(s)

OCAC reserves the right to accept or reject any proposal, and to annul the tendering process/ public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for OCAC action.

8.3 Purchaser's Procurement Rights

Without incurring any liability, whatsoever to the affected bidder or bidders, the Purchaser reserves the right to:

a) Amend, modify, or cancel this tender and to reject any or all proposals without assigning any reason.

b) Change any of the scheduled dates stated in this tender.

c) Reject proposals that fail to meet the tender requirements.

d) Exclude any of the module(s)

e) Remove any of the items at the time of placement of order.

f) Increase or decrease no. of resources supplied under this project.

g) Should the Purchaser be unsuccessful in negotiating a contract with the selected bidder, the Purchaser will begin contract negotiations with the next best value bidder in order to serve the best interest.

h) Make typographical correction or correct computational errors to proposals

i) Request bidders to clarify their proposal

8.4 Notification of Award

Prior to the expiration of the proposal validity period, OCAC will notify the successful bidder in writing or by fax or email, that its proposal has been accepted. In case the tendering process/public procurement process has not been completed within the stipulated period, OCAC may like to request the bidders to extend the validity period of the bid.

The notification of award will constitute formation of the Contract. Upon the successful bidder's furnishing of Performance Bank Guarantee (PBG), OCAC will notify each unsuccessful bidder and return their EMD.

8.5 Contract Finalization and Award

The OCAC shall reserve the right to negotiate with the bidder(s) whose proposal has been ranked best value bid on the basis of Technical and Commercial Evaluation to the proposed Project, as per the guidance provided by CVC. On this basis the contract agreement would be finalized for award & signing.

8.6 Performance Guarantee

a) OCAC will require the selected bidder to provide a Performance Bank Guarantee

(PBG), within 15 days from the date of notification of award.

b) The bidder should furnish PBG amounting to 10% of work order value excluding tax in favour of OCAC valid for 68 months as per format attached at clause 10.3.4

c) The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the service during the work order period.

d) In case the selected bidder fails to submit performance guarantee within the time stipulated, OCAC at its discretion may cancel the order placed on the selected bidder after giving prior written notice to rectify the same.

e) OCAC shall invoke the performance guarantee in case the selected bidder fails to discharge their contractual obligations during the period or OCAC incurs any damages due to bidder's negligence in carrying out the project implementation as per the agreed terms & conditions.

8.7 Signing of Contract

After OCAC notifies the successful bidder that its proposal has been accepted, OCAC shall enter into a contract with the successful bidder (prime bidder in case of consortium), incorporating all clauses, pre-bid clarifications and proposal of the bidder.

A draft MSA document has been provided as a separate document for the reference of bidders only. The agreement with the selected bidder will be signed after getting the same vetted from competent Legal Authority.

8.8 Failure to Agree with the Terms and Conditions of the RFP

Failure of the successful bidder to agree with the draft legal agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of award, in which event OCAC may call for new proposals from the interested bidders. In such a case, OCAC shall invoke the PBG of successful bidder.

8.9 Contract Term

Contract duration would be 66 months from the date of issuance of work order i.e. 6 months of supply, configuration, installation and commission and 60 months of operation and maintenance support from the date of commissioning.

9 SCOPE OF WORK

i The primary scope of this RFP is to procure necessary Cyber forensic tools for the Department to carry out investigation, monitoring, data, evidence analytics and prosecution.

ii The Successful Bidder shall ensure implementation of the proposed cyber forensic tools as per the scope defined in the RFP.

iii The proposed forensics tools, social media Tools and Crime data analytics, equipment's shall provide technical aid in investigation and prosecution and speed up the investigation process.

iv The successful bidder shall need to provide their solutions under these three major components.

- Cyber Forensic Tools
- Cyber Forensic Tools Training to the officers
- Provide manpower to operate the center.
- OSINT & Threat Intelligence Lab
- Awareness, LMS and case studies
- Malware Testing Lab (Digital Twin/Range)
  Deliverable
  a) Detailed design and architecture of the cyber range infrastructure.
  b) Customized cyber range scenarios replicating various cybercrime incidents.
  c) Training modules and materials for digital forensic investigations within the cyber range.
  d) Fully functional and secure cyber range environment for digital forensic lab use.
  e) Integration of necessary forensic tools and technologies within the cyber range.
  f) Comprehensive documentation on the implemented solution and its maintenance procedures.

Note: OCAC / Odisha Police Department shall provide necessary underlying physical & logical infrastructure & facilities required to successfully set up and operate Cyber Forensic hardware and software.

9.1 CYBER FORENSIC TOOLS (PROPOSED)

The below mentioned are the categories for Cyber Forensic Tools.

Computer Forensics	This section shall be fully equipped with the high-end processing workstations, updated versions of forensic tools, legacy equipment etc. This section shall be able to perform the initial processing, data extraction from computer systems and make available the filtered data for further analysis for services related to forensic investigation with deep registry analysis, shadow file analysis, search methods -active files,

	deleted files, slack space, Unallocated space, memory file, Hibernation file, page file, Metadata, registry, Data hiding techniques-Ghosting, file extension changing, encryption, steganography, password protection, Data Carving-file signatures, search-active files, deleted files, slack space, Unallocated space, memory file, Hibernation file, page file, Metadata, registry, Data hiding analysis-Ghosting, Hashing and Authentication analysis etc..
Mobile Forensics	This section shall be fully equipped with the high-end processing workstations, latest versions of forensic tools and equipment's. This section shall be able to perform the initial processing, data extraction from mobile devices and make available the filtered data for further analysis for services related to forensic investigation with to perform hashing, bypass the anti-forensic obstacles, deep scan, data imaging, Physical and Logical data extraction, Data Indexing, Data Carving, Recovery & Analysis, finding the Call Logs, SMS, MMS, Image, Audio, Video, Web, Email, Instant Message/Chat, Web Browsing History, System Logs, Volatile Memory, Cookies, File Documents, Databases, Executable Files, Internet data and Public & Private Cloud artefacts etc.
Audio & Video Footage Authentication and Analysis Section	This section shall collection, extraction, recovery, analysis, and identification of evidence from DVR/CCTV and other device or network sources and perform authentication and enhancement analysis related to Image, Audio and Video.
Embedded Forensics	This section shall collection, extraction, recovery, analysis and identification of evidence from Embedded Systems (IoT, UAV, Smart Devices and Vehicle firmware devices etc.) for memory extraction and analysis using JTAG and Chip off methods.
Network Forensic & Internet Investigation	This section shall collection, extraction, recovery, analysis, and identification of evidence from Internet evidence.
Malware & Incident Investigation	This section shall be capable of performing analysis of malware files for analyses the cyber-attacks in a dedicated Cyber Simulator/Lab. a) Design and set up a fully functional Digital Twin environment suitable for digital forensic investigations. b) Customization of the Digital Twin to replicate diverse cybercrime scenarios, including malware infections, network intrusions, data breaches, and insider threats. c) Development of training modules and scenarios specific to digital forensic investigations, allowing analysts to enhance their skills and knowledge. d) Provision of a secure and controlled environment for forensic analysts to practice investigations, perform analysis, and extract digital evidence. e) Integration of necessary tools, software, and hardware required for efficient digital forensic examinations f) within the cyber range. g) Documentation and training on the operation and maintenance of the implemented cyber range solution.

9.2 Project Kick–Off

During Project Setup & Initiation stage, the vendor will designate a nodal person to serve as the single point of contact for the Project (Project Manager). The project managers will:

i. Develop a Project Schedule
ii. Conduct a Project Kick-Off meeting to introduce all stakeholders
iii. Conduct risk assessment
iv. Deliver Kick-off Presentation
v. Document and Obtain Sign-off on Project Plan

9.3 Deliverables

- Project Inception Report/ Delivery report
- IT Infrastructure Requirements Definition

During this stage, the vendor will coordinate with all stakeholders to gather the requirements:

i. Identify and define installation requirements
ii. Identify and define inter-connection/integration requirements
iii. Any other requirement to complete the scope of work

Schedule Deliverables

No	Items	Site/Location	Timeline in days
1	Supply / Delivery of Software/tools/Hardware of the solution(all mentioned in SOW)	Police Commissionerate Office, Bhubaneswar	T+24 weeks after the issue of the PO
2	Installation and commissioning		T+28 weeks
3	Documentation and manuals	Police Commissionerate Office, Bhubaneswar	Within 21 days of the operational acceptance

The Implementation Agency shall ensure that the solution is thoroughly tested as perthe standard process defined hereunder or by OCAC should the process evolve over the contract period. OCAC requires a thorough and well-managed test methodology to be conducted. The Implementation Agency must build up an overall plan for testing and acceptance of the system, in which specific methods and steps should be clearly indicated and approved by OCAC. The Implementation Agency is required to incorporate all suggestions/feedback provided after the elaborate testing of the IT Infrastructure/Solutions supplied, within a pre-defined, mutually agreed timeline. Bidder shall provide the manpower for installation and commissioning and support for five years from the date of commissioning. OCAC will confirm to depute the manpower for doing this activity if required. There will not be any additional cost for this process.

The Implementation Agency shall undertake the following broad-level activities:

i. Outline the methodology that will be used for testing and fine-tuning the system from time to time
ii. Define the various levels or types of testing that will be performed for the system.
iii. Provide the necessary checklist/documentation that will be required for testing the system
iv. Describe any techniques, test cases/scenarios/scripts that will be used for testing the system.
v. Bidder should prepare and submit SOP of each tool and operational procedure
vi. Describe how the testing methodology will conform to the requirements of each of the functionalities
vii. Indicate/demonstrate to OCAC that all desired Software/Applications/tools installed in the system have been tested.
viii. The vendor shall provide a workflow for sign-off on test deliverables that is mutually agreed by both parties
ix. User acceptance certificate should be provided by the vendor.

Competent Authority from OCAC/ Police Commissionerate Office shall issue an appropriate acceptance certificate to the Implementation Agency for the successful roll-out of the application. The testing levels should include Unit Testing, Integration Testing, System Testing and Acceptance Testing (including performance testing and fine-tuning). These tests should be included such as security testing, performance testing, Usability testing, Concurrency testing, etc. The Implementation Agency must work with OCAC to provide a detailed deployment plan, including but not limited to, application version control, loading all application materials, assignment of user rights and security, and verification ofcorrect functionality.

An Operational Acceptance shall commence on the system, once the system is commissioned for a period of maximum 15 days. Operational Acceptance will only be provided after UAT has been performed, and sign-off on the UAT obtained from OCAC/ Police Commissionerate Office.The implementation agency will have to facilitate the testing of all applications from OCAC users during the operational acceptance.

9.4 Technical Support

- The bidder must provide required support to OCAC/ Police Commissionerate Office after installation and commissioning.
- The bidder (through OEM) must provide training to the selected professionals of OCAC/ Police Commissionerate Office on the quoted products and management.
- The support person (must have hands-on each and every installed tool)/ team shall remain readily available to the OCAC support team on phone/ email and shall be readily available in person to the premises when required. However, if required, OCAC/ Police Commissionerate Office /Govt. may ask the bidder's support person/ team to be available on holidays/ beyond office hours. The bidder shall be required to immediately provide a replacement support person; in case thedeputed person is on leave due to any reasons.
- The bidder should provide the installation and commissioning status report weekly basis.

10 TECHNICAL SPECIFICATIONS

Central Lab Hardware

Forensic Core Server Stack

- Must have 42U Standing Rack cabinet with Server Rack 42 U 2000x800x1000mm RAL7021 and 4 x 19"-power distribution unit 8x C13 + C14-connector 10A,
- Must have built in Dongle Server with minimum 20 Ports.

File Server

- Should have 4U Chassis.
- Should have Dual Socket P (LGA 3647) support 2nd Gen Intel® Xeon® Scalable processors (Cascade Lake/Skylake)‡
- 16 DIMMs; up to 4TB 3DS ECC DDR4-2933Forensicz† RDIMM/LRDIMM, Supports Intel®
- Optane™ DCPMM††
- 4 PCI-E 3.0 x16 (double-width) slots, 2 PCI-E 3.0 x16 (single-width) slots, 1 PCI-E 3.0 x4 (in x8) slot
- 8 Hot-swap 3.5" drive bays
- 2x 10GBase-T LAN ports
- 1 VGA, 2 COM, 5 USB 3.0
- 4 Heavy duty fans, 4 exhaust fans, and 2 active heatsink with optimal fan speed control
- 2200W Redundant Power Supplies Titanium Level (96%)
- USB 3.1 Gen2 front Hub 10 Gbps, USB 3.1 Gen2-Hub und Type C 10. Backplane 4 x 2.5" SSD/HDD
- Should have 2 x 12-Core Intel® Xeon® Silver Processor 4214 (2.20 GHz)
- Should have 2 x Samsung or equivalent 64 GB reg ECC DDR4-2933
- Should have 1 x SSD 2TB M.2 NVMe for the System
- Should have BD/DVD/CD Writer Silent Edition
- Should have 8 x Enterprise 14TB, 512e/4Kn, SAS 12Gb/s for Storage
- MegaRAID 9480-8i8e, 4GB 2133 Forensicz DDR4 SDRAM
- Should have Intel Ethernet Network Adapter, 2x 10 Gigabit
- Should have Windows Server 2019 24 Core
- Must have 1-year warranty
- Must have Backup & Restore utility incl. 500GB USB 3.0 Boot HDD for Initial Installation Recovery

Processing Server

- Should have 4 U Chassis
- Should have Intel X299 Chipset; 8x DIMM with Max. 256GB DDR4 RAM; 2 x Gigabit LAN Controllers; 2 x USB 3.1 Gen 2 Schnittstellen (Type-A + USB Type-C)
- Should have 14-Core Intel® Core™ i9-10940X X-series Processor (3.30 GHz) with active cooling
- Should have 1200WATT Modular Power Supply ATX, EPS12V, PS/2
- Should have 4x 32GB DDR4 RAM, non-ECC
- Should have - HDD-Intern
    - x 2TB SSD M.2 NVMe PCIe for OS
    - x 4TB SSD SATA for Cache
    - x 18TB Enterprise HDD SATA-III for Data
- Should have SMART-UPS 3000VA LCD RM 2U 230 WITH SMARTCONNECT IN

- Should have 8x Backplane for Storage HDD's
- Fully Featured 1U LCD KVM Drawer- OSD KVM - USB + VGA Support
- Control your server or KVM switch from a centralized LCD KVM drawer.
- Should be NVIDIA GPU, min. 4GB memory, PCIe, HDMI/ DisplayPort
- Should have Optical Drives - DVD Blu-ray Writer, SATA
- Should have Controller - 1x 10 Gigabit Ethernet Controller with 1x RJ45 Port
- Should have Forensic-Bridge
    - Tableau T356789iu Forensic Universal Bridge USB3.0&PCIe & SATA & FireWire & IDE & SAS Silent Edition
    - incl. all cables, adapters and cooled Imaging Shelf.
    - Cable Set: TC2-8-R2, TC4-8-R2, TC6-8, TC7-9-9
    - PCIe Adapter Set: TDA7-1, TDA7-2, TDA7-3, TDA7-4, TDA7-7, TCPCIE-4
    - SATA&IDE Adapter Set: TC6-2, TDA3-1, TDA3-2, TDA3-3, TDA3-LIF, two LIF cables, TDA5-18, TDA5-25, TDA5-ZIF, TC20-BNDL
- Should have - Keyboard/Mouse Kit
- Should have - Windows 10 Professional 64-bit, Forensic Software: TIM (Tableau Imager, FTK Imager, and other open source)
- Should have - External bootable HDD with pre-installed Backup Software
- Should be Tested and certified for use with leading forensic tools like AXIOM and NUIX, etc
- Product Should carry 12 months Warranty.

SAN Storage

- Should have RAID Module 432TB gross capacity each JBOD 4U
- Should have Single Expander Backplane Boards support SAS3/2 HDDs with 12Gb/s throughput
    - 4 x Mini-SAS HD ports for Internal / External Cascading Expander Combination for high performance, high availability or high redundancy requirements
    - 1x IPMI port for Remote System Power on/off and system monitoring
    - Support NTP for time synchronization & RTC battery backup
    - 600W (1+1) 94% efficient Platinum level power supplies
    - 5 hot-plug redundant cooling fans
    - Ideal for Cloud backup, data Replication or High desnsity Archive Storage Applications
- Should include 24 x Enterprise 18TB, 512e/4Kn, SAS 12Gb/s
- Should have RAID Controller (Installed in Server module)

Networking

- Should have LAN Switch 48 x 10G + 4 x 40G.
- Should be Data center optimized 10-Gigabit Ethernet switch offering the flexibility of different speeds, 40G, 10G and 1G for smooth cost-effective network migration
- Should have Port Attributes:
    - 48x 10-Gigabit Ethernet ports - RJ45
    - 4x 40-Gigabit Ethernet ports - QSFP+
- Should have - Switching Capacity: 1.28 Tbps
- Should include 10 Gigabit Patch Panel
- Should have a Console with 8-Port KVM Switch
- Should have APC Smart-UPS X 3000 VA, RM, 230 V with 4U
- Tape Archive Module
- Should have 2U Tape Archive Module
- Should be Quantum SUPERLOADER 3 1x LTO8HH 16 SLOTS SAS RACKMOUNT
    - Quantum SUPERLOADER 3 8 SLOT LTO MAGAZINE
    - 12x LTO-8 Drive 12/30TB Backup Software

Password Acceleration Server

- Password recovery cluster performance with up to 69,92 Teraflops and 39936 Cuda Cores
- Chassis: - 4U / Full Tower Chassis Supports max. Motherboard, Sizes – E-ATX 15.2” x 13.2”/
- ATX/Micro ATX
- Must have 8x 3.5” SAS/SATA Backplane for Hot-Swappable Drives (Support SES2)
- Must have 11x Full-Height, Full-Length Expansion Slots Optimized for 4x Double Width GPU Solution
- Must have (2x) Rear Additional 80mm PWM Fans & (4x) Middle Lower 92mm PWM Fans
- Power supply: 2000W Redundant Titanium Level Certified High-Efficiency Power Supply
- CPU: 1x 8-Core Intel® Xeon® Silver Processor 4215 (11 MB Cache, 2,50 GHz)
- RAM: 4x 32GB DDR4-RAM - ECC REG
- System Drives: 1x 1000GB SSD, m.2 for OS
- Graphic cards: 4 x NVIDIA RTX A6000 48GB GDDR6 ECC PCIe 4.0x16 (Quadro)
    - GPU memory 48 GB GDDR6
    - Memory interface 384-bit
    - Memory bandwidth 768 GB/s
    - NVIDIA Ampere architecture- based CUDA Cores 10,752
    - NVIDIA third-generation Tensor Cores 336
    - NVIDIA second-generation RT Cores 84
    - Single-precision performance 38.7 TFLOPS7
    - RT Core performance 75.6 TFLOPS7
    - Tensor performance 309.7 TFLOPS
- Periphery: Keyboard / Mouse Kit
- Windows 10 Professional 64-bit
- *Dual Boot with Windows & Kali Linux is possible on request*
- must be Certified and tested with Passware Kit Forensic and ElcomSoft distributed Password Recovery.
- Should instantly recover many password types.
- Should instantly decrypt MS Word and Excel files for all versions (including Decryptum attack).
- Should reset passwords for Local and Domain Windows Administrators instantly.
- Should recover encryption keys for hard disks protected with BitLocker, including BitLockerToGo.
- Should decrypt TrueCrypt.
- Should recover from 8 different password attacks (and any combination of them) with an easy-to-use setup wizard and drag & drop attacks editor.
- Should use multiple-core CPUs and NVIDIA GPUs efficiently to speed up the password recovery process.
- Should provide detailed reports with MD5 hash values.
- Should be capable of recovering Mac User Login passwords and FileVault2 keys from computer.
- Should support Distributed and Cloud Computing password recovery on both Windows and Linux platforms.
- Should recover passwords for Windows users from a memory image or a standalone SAM file, including UPEK.
- Should recover passwords for email, websites and network connections from standalone registry files in a very short time.
- Should have Search Index Examiner to retrieve electronic evidence from a Windows Desktop Search Database
- Should be able to decrypt passwords for Facebook, Google, and other websites from live memory images or hibernation files.
- Should include Special password recovery attacks such as: Rainbow Tables, Decryptum, SureZip, ZipPlaintext

- Should support Password modifiers (case changes, reversed words etc.)
- The license term for the software must be for a period of 3 years with regular upgrades and updates.
- Must have 12-month warranty & made in Germany.

Forensic Integrated Workbench

- Should be with all necessary forensics modules integrated, forensics hardware, optional forensics software, high performance workstation and touch screen panel.
- The workflow and regulations of digital forensics are built within the work process which can reduce the workload and errors.
- Integrated with all mature forensics technology & products, easy for maintenance and update.
- Apply automated forensic tasks with customizable procedures. Investigators will no longer be occupied by manual operations but focus more on data analysis.
- instead.
- Human oriented design provides a comfortable and friendly experience when a forensics work is executed.
- Support parallel processing to improve work efficiency.
- System Specification
    - Intel C621 Chipset
    - Intel Xeon Gold 5218 16 Core Processor 2.3 - 3.9GHz * 2
    - 1TB DDR4 2666Forensicz ECC REG Memory (16 x 64GB)
    - 2TB SSD SATA III HDD (operating system with win 10 Pro - 64)
    - 2TB SSD SATA III HDD (Temp/Cache/DataBase)
    - 32TB (8TB x 4) SATA Hard Drive for data
    - Nvidia RTX 3050 8GB GDDR6 3DP 1HDMI Video Card
- Write-blocker Interfaces
    - Type C (USB3.1) write blocker x 2
    - 3.5” SATA/SAS x 4
- Read/Write Interface
    - USB 3.0 Type A x 10 port (power independent)
    - 3.5” SATA/SAS port x 4
- Multi interface Write blocker with
    - PCI-E x 1
    - SATA x 1
    - USB 3.0 x 1
    - IDE x 1
    - SCSI x 1
    - Write Blocked port: Media Card Reader port(support TF/M2/SD/MMC/MS/XD/CF)
- Single RAID Chassis Option:
    - PCI-e Standard Expansion Slots
    - One (1) 2.5" Bay with 2 Removable Trays
    - One (1) 3.5" Bay with 3 Removable Trays
- Module
    - Built-in Wireless charger x 1
    - DVD R/W Driver x 1
    - 2x RJ45 Gigabit Ethernet LAN ports /1x10G fiber
    - 3.5 earphone jack x 2
    - WiFi and Bluetooth module x 1
    - 7.1 Channel High Def Audio-Back Munted
- Dimension: 1600(L) X 800(W) X 750(H)mm (890mm at the highest point)

- Built-in rear speaker
    - Digital Camera Built-in HD Camera for evidence recording
    - Control access Built-in 14" touch screen
    - Power adapter 1800W
- Software:
    - Duplication Software with Hashing
    - Win 10 64bit English Version and Novell SUSE Linux Enterprise
- Display:
    - Samsung or equivalent 34 inch Curve 21:9 with 1800R WQHD 3440 x 1440 (2K) - 100Hz, Type-C port.

Forensic High end workstation

- Should have 10-Core Intel® Core™ i9-10900X X-series Processor (19.25M Cache, 3.70 GHz - 4.50 GHz) with active liquid cooling
- Chassis: Must be a Big Tower Case: 306(W) x 651(H) x 639(D)mm
- Should have RAM 64GB (expandable up to 256GB)
- Should have
    - 1 x 1TB SSD M.2 NVMe PCIe for OS
    - x 1TB SSD M.2 NVMe PCIe for Temp
    - x 4TB SSD M.2 NVMe PCIe in RAID0 via vroc
- Should have Integrated Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface
- Should have NVIDIA GTX1660. 6GB memory, PCIe, HDMI/ DisplayPort
- Must have Retractable cooler for suspected drive
- Should have 10/100/1000 Mbs Gigabit Ethernet Network Adapter
- Should have 1 PCI-Express 3.0(x16)Slot
- Digital Optical S/PDIF audio output
- Should have 1 RJ45 LAN port (Gigabit LAN controller)
- Should have 802.11a/b/g/n/ac WiFi+ Bluetooth 4.0
- Should have 1x USB 3.1 Typ-C; 4x USB 3.0 Typ A front Mounted
- Should have 2x USB 3.1 ports (1 port at Type A, 1 port at Type C) Back Mounted
- Should have Keyboard and Mouse Combo
- Should have Adapters and Cables: Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8 inch IDE (iPod), 2.5 inch IDE (laptop), PCIe Card SSD Adapter, PCIe M.2 SSDS Adapter, PCIe Apple SSD Adapter and PCIe Cable
- Should have Windows 10 Professional 64-bit, Forensic free Software: TIM (Tableau Imager, FTK Imager, other Imager)
- Should have an External bootable HDD with pre-installed Backup Software
- should be Tested and certified for use with Encase Forensic, AXIOM and NUIX
- Product should carry 1 Years On-Site Warranty. Any Software/ Firmware updates to be provided during the Warranty Period.

Forensic Parellel Data Extraction -Multi channel Mobile Analyzer and Charging station

- 15U - 19-inch cabinet with 40cm depth
- Cabinet external dimensions 60x75,8x40 (WxHxD)
- Mounted on trolley with 4 castors and brake
- Removable lockable side walls
- lockable front door made of ESG safety glass

- Seven steps for storing the smartphones
- Space for five devices per level
- Anti-slip strips at device positions
- Gradually offset device positions for better access
- Charging cable feeders from below
- Recesses in the perforated sheet tapered downwards for plug catching
- Roof fan with quiet fans, temperature controlled with thermostat (setting range: +5 °C... +60 °C)
- Equipped with 2x 8-way power strip
- WLAN smoke detector with app notification incl. 2x batteries
- Chargers for 35x tablets, smartphones and other devices
- 35x Apple iPad/iPhone/iPod/MacBook data cable/charging cable (Apple Lightning plug)
- 35x USB-C 3.0 Label Cable
- A new generation of mobile forensics, with high speed simultaneous extraction and analysis of cell phones, tablets and GPS devices. Can extract deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from the Cloud Apps and many others with only A few clicks.
- Should include with Hardware:
    - Intel Core i9-11900 Processor
    - 2x 16GB DDR4 RAM
    - 500GB SSD M.2 NVMe PCIe for OS
    - 2TB SSD M.2 NVMe for Data
    - 7-Port USB 3.1 Gen 2 Hub with 4x A-Ports and 3x Type-C Ports
- Supports 8-channel analysis of cell phones using Parallel Forensics Technology.
- The easy to use GUI that allows you to view extractions and see prgress at the same time, with its function for viewing multiple contents and its network signal shielding module to shield signal between host and cell phones to remove any external interference.
- Decrypt cell phone applications with the advanced GPU technology of powerful computers.
- Supports the emulation of Android smart phones for the discovery of more data from clouds, the analysis of user behavior on applications and much more.
- Should have phone and cloud extractor, data analyzer and report generator all in one solution.
- should include with 12 month warranty and support

Central Lab Software

- The offered Solution should enable to organize, manage, and report on all aspects of a digital forensics investigation while upholding the chain of custody.
- The offered solution should come with 25 users and option to scale in the future. All users can be individually assigned roles of executives, managers, or contributors depending on intended access level.
- Should allow Examiners to add the read-only users on a case-by-case basis to the dissemination list, by using the restricted access utility.
- Should track all evidence sources, examinations, and individuals who came in contact with digital evidence—ensuring that the full case history is preserved.
- Lab managers should be immediately notified when a web form is submitted and can assign the appropriate resource to the case.
- Should enhance collaboration and make it easy for any team member to kick-off and contribute to a digital forensic investigation, ensuring that everyone stays in-the-loop—no matter where they are located.
- Should report on the following and more:
    - The number of evidence sources reviewed per case/month/year.
    - The examiner-hours spent on each evidence item or case.
    - The number of cases assigned to each investigator

  - The forensic tools and hardware used on each investigation.
- Tool should be collaborative end-to-end product that uses a clean, intuitive interface, allowing anyone get started with very little training. It should provide digital evidence and lab management, as well as archiving, which allows teams to understand how the evidence was handled and where to find it in the future.
- Should support assignment of roles to users as executives, managers, contributors, Read-Only Limited, Read Only system, Supervisor, Authorizer, Affiliate, Recipient etc depending on intended access level.
- Tool should works through common browsers on Windows, Mac, Linux, and mobile OSes and it builds statistics as you enter information. It should be able to incorporate case management stats into reporting tools.
- The solution should also have below features:
  - Global Collaboration on Any Case
  - Unlimited Client Base certificate.
  - Permanent Case Archives
  - Chain of Custody Preservation
  - Complete Exam Documentation
  - Curriculum Vitae Management
  - Asset Management
  - Local or Remote Browser Access
  - Consolidation of All Case Information
  - Automatic Statistics Generation
  - ICAC and Cyber tip Management for Law
  - Financial Information Management
  - Lab Expenses Analysis
  - Grant Documentation Management
  - Project Expense Accountability
  - Invoice Generation
  - Process Review Facilitation
  - In- eld Evidence Triage
  - Scalability to Grow with Your Needs
  - Barcode Generation
  - Secure 256-bit Encryption
  - Standardized, repeatable process management
- Should ensure agency data security With role-based permissions, password protection, AES 256-bit encryption for data at rest, and TLS/SSL encryption for data in transit.
- Should have option for Read-only users to submit requests for services through a submission form. Using the submission form should be an option that may be enabled/disabled in Settings.
- Should allow examiner to take Case notes, Item notes and Examination notes to support fully documenting an investigation.
- Should have Request Tab, Incident Details Tab, Details Tab, Case Note Tab as a case creation option.
- Incident Tab which describes the incident should have the following fields Begin Date, Ending date, Indent response timing tools, Incident Location, Offense, Suspect and Victim etc.
- Details Tab should have the following fields; Initiation Dates, Purge Date, Case Year, Reporting Period, Case Status, Case Types, Origin, Case Procedure, Locations, Case Tags, External Findings etc
- Should have API support to integrate and connect with other tools in your existing ecosystem to trigger key tasks such as creating a new case, adding evidence to a case, pulling aggregated statistics, and more.
- Case Page should have an option to categorize cases into Unassigned, Assigned, View, Pending Approval, remove case, Define Access etc.

- Every record should have its own access list to restrict access to certain records within a case.
- Should have timeline view on the case page to present a chronological history of all notes entered on any of the records within the current case. Should have an option to select the "Views" selector to select or deselect the Chart, Details, Summary, Timeline, and Totals views.
- Should have Evidence, Case & Expense Reporting feature to makes it easy to generate both the real-time and historical statistics you need to build reports for stakeholders and keep a holistic record of digital forensic examinations to review prior cases and quickly pinpoint areas of interest.
- Should support Assets management to allow the user to describe the tools they use during their work phases and to facilitate the management and tracking of those assets. Assets should be recorded on case work by selecting assets within the “Connected Hardware” and “Connected Software” fields while editing the Items.
- The assets section should also manage the existence, inventory, assignments history, and financial information related to these tools. By utilizing the assignment utility for assets, inventory control should be accomplished by filtering by several criteria including assignees and teams.
- Should support Personnel management by establishing personnel formal education, Job experience, Courses they are linked etc. This action permits the update of training records by linking one or more attendees to a single course.
- Should allow stakeholders to easily review past investigations to ensure that appropriate procedures were followed.
- The case leader should have the capability to submit the case for Quality Assurance review and should have a modal to notify the intended reviewer(s) as well as the investigating read-only submitter the case is ready for the approval process.
- creates a db snapshot and hash of the case at submission for QA review. When the case is approved another snapshot and hash should be recorded. The case compliance audit utility should allow users to see any differences in the case from the time it was submitted to the current moment it is being viewed, any differences from the time it was submitted until it is approved, and from the time it was approved to any time the case is being viewed after approval.
- Should allow stakeholders to Quickly produce reports on your investigations to ensure that appropriate procedures were followed.
- Label printing for evidence items should be available from the individual item pages. The label should prints to any locally installed label printer. A QR code on the label may be used for inventory control if scanned with a 2D scanner to produce a “Scanner file” for comparison in the Audits section.
- Should support creating of Stats on case types, origins, case locations, personnel and more. Time focused statistics can be separate or in addition to the topically based filtered stats by using the date filter. Case filtered statistics provide the widest view of overall work within the system.
- Should support Backlog metric which relates to evidence within open status cases which have no associated examinations that have an exam device type defined.
- backlog number should be displayed beside the Backlog label including the total number of evidence items within open cases with no associated examinations. The chart should display the items based on the item device type defined by the user.
- Should support case urgency metric where investigators can select the Urgency indication based on the list created by Executive users in settings. The urgency metric should display a chart indicating the urgency selection for all open cases. The urgency selection on a case can be edited by the examiner(s) working the case.
- Should support Activity feed which allows users to create dynamic chart that users may filter to focus the feed more closely. The filters should allow users to filter by time periods, by users on the case, by source records types, and by the actions. These should be multi-select filters which

can be chosen in any combination to present the information topically and quantitatively as needed.

- Tool for workflow orchestration and automation to help Digital Forensic Units create a more efficient lab workflow to improve service to the agency, maximize lab investments by utilizing computing power and forensic tools 24 hours a day, 7 days week, and ensuring case quality through consistent workflows and adherence to SOPs.
- The ability to complete a single task without human intervention, making time-sensitive processes more efficient, accurate and reliable to help frees up more time for examiners to spend on high-value tasks that require human review, reasoning, and analysis.
- Orchestration to enable labs to more easily manage and control complex workflows that utilize many different tools, hardware, and processes — maximizing efficiency and reducing overall investigation costs.
- Automated workflow creation and management for digital forensics investigations.
- Drag-and-drop workflow builder to develop efficient, automated workflows.
- Integration with custom scripts for increased flexibility.
- Empowering expert examiners to design workflows for each case type to adhere to standard operating procedures.
- Junior members of the team can kick off the right workflow from a dropdown menu, while experts focus on analysis.
- Ability to process digital evidence 24/7/365, utilizing computing power and forensic tools continuously.
- Building prioritized job lists to ensure continuous imaging and processing of evidence items.
- Ability to process large volumes of data with high speed and accuracy.
- Scalability to accommodate growing business needs.
- Minimal system downtime and efficient use of system resources.
- Integration with any tool from the forensic toolkit, including mobile acquisition tools.
- Provides flexibility to adapt to evolving lab needs and changing industry standards.
- Should support Mapping a CSE triage workflow for use as a first pass on all devices seized. Deliver consistent outputs with more speed and less effort, including case creation files for media review, grading and AI models on powerful servers.
- Should help Program a quick triage scan to create standardized outputs allowing you to focus the next stage of your investigation more accurately as part of a digital investigation strategy.
- Should support Bulk processing of mobile device images acquired by third party tools, create extra capacity within the lab.
- Should support Utilizing a low-code solution means anyone (who has permission) can create automated workflows even if they don’t know how to script. easy-to-use drag and drop interface, with the ability to add in your custom code if needed.
- Should allow users to create their own Certificate Authority (CA), which generates a CA-signed public certificate and server certificates.
- Should provide clear, visual dashboards to quickly assess lab infrastructure health.
- Provides customizable dashboards and reports to fit users' specific needs.
- Should allow users to create their own metrics and KPIs to measure lab performance.
- Should provide key insights for smarter resourcing decisions.
- Should provide reporting to management on the value of lab investments by tracking overall throughput and efficiency metrics.
- Should provide Data mapping and transformation capabilities.
- Should provide Advanced reporting and analytics.
- Should provide Error handling and logging functionality.
- Should provide User authentication and authorization with role-based access control.
- Should provide Secure transmission and storage of data using encryption protocols.
- Should provide Audit logging and monitoring of system activity.

- Should provide New examiners can begin learning high-value tasks immediately – deriving meaning and satisfaction from their work, while getting up to speed quickly.
- Should provide Informative, visual dashboards can provide instant snapshots of available infrastructure and efficiency metrics that can inform resourcing, funding and talent planning.

Technical Specifications for Computer Forensic

Forensic All in one for Computer + Mobile + Cloud

- Use automation to queue multiple devices and device types for image acquisition.
- Layer filters and use multiple views to surface the most relevant results
- Find artifact data, file system data, and registry data – including unallocated or deleted space
- Analyze using multiple views, filters, searches, categories.
- Link artifact data back to its file system or registry source data in seconds.
- Share a Portable Case
- Find, analyze and report on the digital evidence from computers, smartphones and tablets.
- Find Internet Explorer, Chrome, Safari, Firefox and others browsers activity
- Find forensic artefacts from instant messaging and chat applications like skype, google talk, Facebook, twitter etc.
- Find forensic artefacts from cloud drives like dropbox, Flickr.
- Identify important evidence quickly by searching for specific keywords.
- Create keyword lists to get real-time notification on hits while a search is processing.
- Isolate evidence from a specific date or time range or create filters to narrow results based on field values for any supported artifact type.
- Visualize digital evidence in an organized and chronological sequence.
- See all geo-location evidence for a case plotted on a world map.
- Identify and categorize images recovered by an IEF search with built-in picture and analysis tools: Refine results using skin tone filters, View PhotoDNA, MD5 and SHA-1 hashes for recovered files, View PhotoDNA, MD5 and SHA-1 hashes for recovered files, import hash values from Project Vic or custom hash databases to quickly identify and categorize illicit images
- Re-create a visual representation of a chat thread as it would have appeared in the chat application.
- Rebuild web pages in their original format on the date they were visited.
- Export reports in a variety of formats including, PDF, Excel, CSV, XML and tab-delimited formats.

Evidence Centre Software

- Easy for an investigator to acquire, search, analyze, store and share digital evidence found inside computer and mobile devices, RAM and cloud.
- Quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, cloud, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps.
- automatically analyze the data source and lay out the most forensically important artifacts for investigator to review, examine more closely or add to report.
- Discovers more than 800 types of artifacts, including over 100 mobile applications, all major document formats, browsers, email clients, dozens of picture and video formats, instant messengers, social networks, system and registry files, P2P and file transfer tools, etc. Extracts data from all major operating systems, both computer and mobile: Windows, Linux, MacOS X, iOS, Android, Windows Phone, Blackberry.
- Looks for hidden and encrypted information, searches in unusual places, carves deleted and damaged data and examines files in little-known formats to discover more evidence than ever.

The search includes unallocated and slack space, $MFT, $Log, Volume Shadow Copy and other special and little-known areas of operating systems.

- allows you to perform evidence search faster than most tools as it does not index every single file found on the data source, instead searching for the most forensically significant types of artifacts. Efficient usage of CPU adds to speediness of processing, as does the code written by our team of highly qualified specialists in data analysis.
- Recovers corrupted and incomplete SQLite databases, restores deleted records and cleared history files. Processes freelists, write-ahead logs and journal files, and SQLite unallocated space.
- extract potentially crucial information from volatile memory, such as: in-private browsing and cleared browser histories, online chats and social networks, cloud service usage history, and much more.
- Equipped with File System Explorer, Hex Viewer, and Type Converter
- Free scripting module allows user to write their own custom scripts in order to automate some of the routine and further extend the product's functionality.
- Supported picture formats:3FR, ARW, BAY, BMP, BMQ, CAP, CINE, CR2, CRW, CS1, CUT, DC2, DCR, DDS, DIB, DNG, DRF, DSC, EMF, ERF, EXIF, EXR, FAX, FFF, G3, GIF, HDR, HEIC, IA, ICO, IFF, IIQ, J2C, J2K, JFIF, JNG, JP2, JPE, JPEG, JPG, K25, KC2, KDC, KOA, LBM, MDC, MEF, MNG, MOS, MRV, NEF, NRW, ORF, PBM, PCD, PCT, PCX, PEF, PFM, PGM, PIC, PICT, PNG, PNM, PPM, PSD, PTX, PXN, QTK, RAF, RAS, RAW, RDC, RLE, RPBM, RPGM, RPPM, RW2, RWZ, SGI, SR2, SRF, STI, TGA, TIF, TIFF, WBM, WBMP, WMF, XBM, XPM.
- Picture analysis allows detection of texts, faces, and skin tone. Detection of photo manipulation (forgery) is available with Forgery Detection plugin (extra module)
- The following formats can be carved: GIF, JPEG/JPG, PNG, BMP, WMF
- Supported video formats: 3GP, 3G2, ASF, AVI, DIVX, DRC, F4A, F4B, F4P, F4V, FLV, IFO, M2V, M4P, M4V, MK3D, MKA, MKS, MP2, MP4, MKV, MOV, MPE, MPEG, MPG, MPV, NSV, OGG, OGV, QT, RM, RMV8, SVI, TS, VOB, WEBM, WMV
- Key frame analysis available for 3GP, 3G2, AVI, MP4, MPEG, MPG, WMV, MOV videos
- Social Networks: Bebo, Facebook, Facebook Messenger, Google+, Myspace, Odnoklassniki, Orkut, Twitter, VKontakte
- Cloud Services: Dropbox, Flickr, Google Drive, SkyDive, OneDrive, Yandex Disk
- Multi-user Online Games: Karos, Lineage, World of Warcraft

Technical Specifications for Computer Forensics software

- The solution should have a timeline view option to provide an easily to search adjustable, graphical calendar like display for file activity of particular interest.
- The solution should contain Full Unicode support to allow users to search text and fonts from any foreign county and in any language.
- Should support acquisition Restart facility: continue a window acquisition from its point of interruption.
- Should have inbuilt utility to acquire evidence via boot Disk.
- Should have inbuilt utility to acquire RAM evidence.
- Should do image verification by CR and MD5.
- Should have Inbuilt support for writing scripts & should have pre-built scripts.
- Should support more than 150 Filters and Conditions.
- Should support combining filters to create complex queries using simple “OR” or “AND” Logic.
- Should have Inbuilt Active Directory Information Extractor.
- Should be able to automatically rebuild the structure of formatted NTFS AND FAT volumes.
- Should support Recovery of deleted file/folders.
- Should have Inbuilt windows event log parser, Link file parser to search in unallocated space.

- Should have Inbuilt support for Compound (e.g., zipped)
- Should have native viewing support for 400 file formats.
- Should have built-in Registry Viewer.
- Should meet the mentioned criteria for searching Unicode.
- index search, Binary search, Proximity Search, Internet and
- emails search, Active Code Page: keyboard in many
- language, Case Sensitive, GREP ;Right to Left Reading, Big
- Endian/Little Endian, UTF-8/UTF-7, Search file slack and
- unallocated space etc.
- Should support Internet and Emails Investigation for: Browsing History Analysis, WEB History & chche analysis, Kazaa toolkit, HTML carver, HTML page reconstruction, Internet artifacts, Instant Messenger toolkit - Microsoft Internet Explorer, Mozilla Firefox, Opera and Apple Safari.
- Supports file signature analysis.
- Should include system support for:
    - Hardware and Software RAIDs
    - Dynamic disk support for Windows Server
    - Interpret and analyze VMware, Microsoft Virtual PC, DD and
    - SafeBack v2 image formats.
    - File System: Windows FAT12/16/32, NTFS; Macintosh HFS, HFS+; Sun Solaris UFS, ZFS; Linux EXT2/3; Reiser; BSD FFS, FreeBSD's Fast File System 2 (FFS2) and FreeBSD's UFS2; Novell's NSS & NWFS; IBM's AIX jfs, JFS and JFS with LVm8; TiVo Series One and Two; CDFS; Joliet; DVD; UDF; ISO 9660; and Plam.
- Should support reporting facility with:
    - Listing of all files and folders in a case
    - Detailed listing of all URLs and corresponding dates and times of web site visited
    - Document incident response report
    - Log Records
    - Registry
    - Detailed hard drive information about physical and logical partitions
    - View data about the acquisition, drive geometry, folder structures and bookmarked files and images
    - Export reports in Text, RTF (opens in Microsoft Office), HTML. XML or PDF formats.
- Should have reporting feature to quickly share a report with organization officials and with a few simple clicks select the exact information for the report and generate an easy to review HTML report that can be viewed in any web browser

Technical Specifications for Mobile Forensic

MOBILE DEVICE EXTRACTION All in one

- The advanced mobile forensic solution should allow you to access the most challenging and secure devices, as well as perform unlimited unlocks and extractions using state-of the-art unique exploits.
- The advance mobile forensic solution should adhere to the fundamentals of digital forensic principles:
- A secured data file container to avoid allegations of interference with electronic evidence after extraction.
- An audit log to show exactly what functions the forensic tool performed on the digital device;
- Hash Algorithm options for enhanced file security and cross referencing;
- To provide password protection on extraction data;
- Examinations should not assume file extentions can be relied upon and instead it should only read the raw digital data.
- The advance mobile forensic solution license should be perpetual license allowing the user organization to keep using the solution at the last version available at the moment of license expiry without any subsequent maintenance from the OEM such as software and hardware updates, hardware warranty, support, etc.
- The advanced mobile forensic solution should allow for the extraction of at least up to 3 mobile devices simultaneously with just a single license key if required.
- The advance mobile forensic solution should be independent of any vendor-specific extraction hardware component(s) that could act as a single point of failure and potentially block the organization's capability of extracting mobile device data in case of malfunction of such component.
- The advance mobile forensic solution should use Windows Certified and signed USB drivers to avoid interference with any other software running on the computer and for IT Security, this information must be available on Microsoft's windows compatible product list. https://docs.microsoft.com/en-gb/windows-hardware/drivers/develop/signing-a-driver
- The advanced mobile forensic solution should provide the capability to perform advanced, forensically sound techniques to extract and decrypt the data from selected devices such as Samsung S7-S10, A10-A50, Samsung Galaxy S8/S9/S10/S20 etc. It should support Ram Brute Forcing Exploit of phones such as Samsung S21, S22, Pixel 6 & 7 and more.
- The advanced mobile forensic solution should provide the capability to extract and decrypt data from devices such as Samsung, Qualcomm, Huawei Kirin, Xiaomi Qualcomm, Oneplus Qualcomm, LG Qualcomm, Google Pixel's and various other Android devices.
- The advanced mobile forensic solution should provide the capability to extract and decrypt the data from various MediaTek chipset-based devices. Support must include (but not limited to) the following chipsets must include (but not limited to) the following chipsets: MT6893, MT6833V, MT6765V, MT6761, MT6762D, MT6833P, MT6785V, MT6762G etc.
- The advanced mobile forensic solution should identify, extract and decrypt Samsung Secure folder.
- The advanced mobile forensic solution should identify, extract and decrypt Huawei Private Space.
- The advanced mobile forensic solution should be able to extract Huawei devices with Kirin processor using brute-force/ Bypass.
- The advanced mobile forensic solution should be able to Unlock Samsung Secure startup using brute-force for Qualcomm.
- The advanced mobile forensic solution should automatically generate an audit trail of the forensic process for peer review.
- The advanced mobile forensic solution should support data extraction from various cloud data sources.

- The advanced mobile forensic solution should have a tool kit for opening of phones. It should also include Huawei & Harmony pro Cables and should have an advanced Pro-Tech Tool Kit.
- The advanced mobile forensic solution should have a dedicated USB high-definition camera.
- The advanced mobile forensic solution should have provision of unlimited extractions.
- The advanced mobile forensic solution should be regularly updated with new releases containing updates to device and app support as part of the license.
- The solution must be able to import Python Script to assists on the decoding and analysis.
- The solution must be able to provide Connection (Link Analysis) View Visualization, Timeline View Visualization, Geographical View Visualization.
- The solution must have text translation & analysis to translate foreign language text on the fly without internet access with additional semantic analysis capability in order to categorize the meaning of specific words, such as categories of abuse.
- The solution must have offline maps to use offline copies of all geographic maps available for our solution and stored locally on PC hard drive.
- The solution must be able to provide PLIST, XML & SQL Database Viewers.
- The solution should have options for export of data into the standard file formats of XLS, XML, PDF, WORD, GPX, KMZ, VIC, FILE, EXTENDED XML, HTML, OpenDocument Text, OpenDocument Spreadsheet.
- The solution should have a content recognition capability and utilising NVidia GPUs to accelerate image classification times.

  The solution should have case review tracking functionality to keep track of case review progress.

Technical Specifications for Computer with Mobile Forensic

- Confidently capture evidence on any mobile device with support for cell phones, GPS and other IoT-associated devices.
- Review, analyze, bookmark and report on all relevant mobile evidence within a single framework to accelerate investigations.
- Review, analyze, bookmark and report on all relevant mobile evidence within a single framework to accelerate investigations.
- Share findings clearly with other investigators, law enforcement, HR, IT and security using a variety of reporting options.
- Share findings clearly with other investigators, law enforcement, HR, IT and security using a variety of reporting options.
- Leverages keyword searches to locate, extract and analyze graphic file text data for a comprehensive view of the evidence.
- Leverages keyword searches to locate, extract and analyze graphic file text data for a comprehensive view of the evidence.
- Conveniently analyzes and reports on evidence in an investigator’s preferred language, including Spanish, French, Polish, Chinese and English.
- Conveniently analyzes and reports on evidence in an investigator’s preferred language, including Spanish, French, Polish, Chinese and English.
- Captures the widest variety of evidence types, including SQLite, Plists, archives, PDF and HTML.
- Utilize workflows that enable review of both parsed and unparsed applications with an interface that models how data should appear from a mobile perspective.
- Find evidence in the most popular cloud-based applications, such as Facebook, Twitter and Amazon, at no additional cost.

Technical Specifications for forensic 8 channel Mobile Analyzer

- Should be a new generation of mobile forensics, with high speed simultaneous extraction and analysis of cell phones, tablets and GPS devices
- Should have ability to extract deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from apps such as Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Signal, WeChat and many others with only a few clicks.
- Should be able to find passwords to encrypted device backups and images
- Should be able to bypasse screen lock on popular Android OS devices
- Should be able to acquire data from cloud services and storages
- Should be able to extract flight history and media files from drones
- Shoould be able to acquire data from IoT devices and smartwatches
- Should be able to provide social links analysis and Timeline view
- Should be able to Collect user data on Windows, MacOS and Linux PCs
- should have Wireless charging station in the device
- Should support 8-channel analysis of cell phones using Parallel Forensics Technology.
- Should have IN WIN A1 Mini-ITX Case with 600 Watt Power supply
- Should have 8-Core Intel® Core™ i9-11900 Processor with 16M Cache, 2.50 GHz - 5.20 GHz
- Should have Corsair Cooling Hydro Series H45 Watercooling + CORSAIR Commander PRO, Digital Fan & RGB Controller
- Should have 32 GB RAM
- Should have 1 - 500 GB SSD and 1 - 2 TB SSD Drives
- Should have 2x USB 3.1 (Gen2) Metall HUB mit 4 Ports 2 x USB-C und 2 x USB-A Anschluss
- Must have a Collection of carefully selected cables covering majority of phones that have ever been on a market
- Should have 1 years Warranty and Support

Technical Specifications for Chinese Phone Extractor

- The perfect data extraction tool for diverse mobile and digital devices
    - Data acquisition for various global smartphone manufacturers (Samsung/Apple/LG/HTC/ZTE) models
    - Chinese manufactured devices (Huawei/Xiaomi/Oppo/Vivo, etc.)
    - IoT device, AI Speaker, Drone, and Smart TV
- Supports Bootloader, Fastboot, MTK, QEDL, Custom Image Android Rooted, iOS Physical, DL, JTAG, Chip-off, SD Card, Removable Media
- ADB Pro extraction which supports data acquisition using vulnerability attacks from Android-based devices
- JTAG pin map viewer and connection scanning with AP
- IoT device data extraction
    - Smart Band - Fitbit
    - Smart Watch - Apple Watch(iOS), Galaxy Gear(TizenOS)
    - SmartTV - Samsung(TizenOS), LG(WebOS)
    - AI Speaker - Amazon Echo, Google Home, Kakao Mini, Naver Clova, KT Giga Genie, SK NUGU
    - ·Drone - DJI (Phantom, Mavic), Parrot, PixHawk
- Advanced logical extraction
    - Android Live, MTP, iOS full filesystem Backup, Vendor backup protocol, Local backup, USIM
- Supports extraction and unlocking of the latest Asian phone

    - Physical extraction through all lock bypass (KNOX, FRP/OEM, Screen Lock): Samsung Galaxy S/J/A/Note series
    - Unlock screen: Samsung Galaxy S/J/A/Note series
    - ADB Pro physical KNOX bypass – Samsung Galaxy S/J/A/Note series
    - Vendor Backup protocol extraction – Samsung, LG, Huawei
    - Local backup extraction - Huawei, Xiaomi, Oppo, Gionee
    - Physical extraction for Japanese manufacturer model - Sharp, Sony
- Supports the latest iPhone logical extraction
    - ·iOS keychain
    - ·iOS full filesystem
    - ·Logical extraction for iPhone up to XS/XR model
    - ·The decryption of backed up data for the latest version of the iOS device
- Useful extraction options
    - ·User-defined extraction for unlisted models using pre-defined methods
    - · Selective extraction by the partition, file, category, app for privacy protection
    - ·Auto-recognition and decryption of partition table and encrypted partition
    - ·Automatic firmware restoration and retrial after restoration failure
    - ·Pause/Resume feature
    - ·Merges multiple image files – MDF and binary file
    - ·Creates MDF file from PC backup
- Assures evidence data integrity
    - ·Write-protection for every piece of evidence
    - · Supports ten different hash algorithms, including MD5, SHA1/224/256/384/512, RIPEMD128/160/256/320
- Support multiple device extraction
    - ·Supports both simultaneous and sequential extraction
- Supports diverse physical data reading hardware
    - ·JTAG Reader (MD-BOX)
    - ·Memory Chip Reader (MD-READER)
    - ·SD Memory Reader/USIM Reader
- Data preview and saving features
    - ·Extraction data preview- Hex viewer
    - ·Sound alarm and TTS alarm for extraction status change
- User-friendly and intuitive user interface
    - ·Intuitive graphical user guide for each extraction method
    - ·Features ‘Recently Selected Models’ List
- Report generation
    - ·Extraction information - Hash value, Time, Method and Filename
    - ·'Extracted File List' generation with a hash value of each file
    - ·Generates ‘Witness Document'
- Supports wide variety of mobile operating systems and devices
    - ·Feature phones, Smartphones and various other digital devices
    - ·iOS, Android, Windows, TizenOS and other mobile operating systems
- Parsing and recovery of various filesystems
    - · FAT12/16/32, exFAT, NTFS, ext3/4, HFS+, EFS, YAFFS, FSR, XSR, F2FS, VDFS, XFS filesystems
    - ·Data carving of unused areas
- Supports analysis of mobile data over 2,000 popular mobile apps
    - ·Multimedia files taken by device camera
    - · Call logs, Address book information, SMS/MMS messages, emails, Memos, and Internet history
    - ·Social networking, maps, navigation, banking, health, and lifestyle apps

    - ·Detection of Anti-forensic apps, and hidden apps
- Supports decoding screen lock and password information
    - ·Decoding unlock patterns, PINs, and passwords
    - ·Brute force through GPU acceleration
    - · iPhone keychain data analysis – Credential (collected from iOS keychain, iOS, App information) can be exported and analyzed
- Data decryption
    - ·Identifying encrypted documents
    - ·Supports decryption of chat messages, emails, files, and other app data
- Deep analysis on popular messenger apps
    - ·Deserialization, decryption, and recovery of data
    - · Skype, Facebook messenger, Telegram, Wickr, QQ, KakaoTalk, Line, Zalo, Viber, Snapchat, and many more
    - ·WhatsApp – Multiple backup file analysis
    - ·WeChat – Multiple account analysis, rainbow table analysis
- Multimedia data recovery and analysis
    - ·Supports frame recovery for deleted/damaged video files
    - · Supports the use of Reference Data Set (RDS) for excluding over 9.8M known unusable images from analysis result data
    - · Supports audio file conversion (From AMR/AUD/QCP/SILK to MP3/AMR/WAV)
    - ·Supports playing QCP files and SILK-encoded audio
- Log analysis
    - · Supports analysis of various logs: media, search word, system, and network logs (Bluetooth, WiFi, Cell towers)
- Social relationship analysis
    - ·Provides Basic/Advanced modes for analyzing single/multiple phones
    - ·Call history, messenger, and email communication data analysis
    - ·Filtering by app, time period, contact(s), and type(s) of communication
    - ·Community analysis
    - ·Relationship visualization and automatic re-organizing
- Embedded data viewers
    - ·View extracted data and source information directly in-application
    - · SQLite databases, HEX, PLists, Documents (Text, XML, PDF, MS Office), Photos, Videos, and Audio
- Visualization of analyzed data
    - ·Map viewer for GPS and cell tower location data
    - ·Offline / Online map (Region / Country / City view levels)
    - ·Timeline view
    - ·Link viewer (social relationship visualizer)
    - ·Chat viewer
    - ·Web browser view (for internet browsing history)
- Advanced data filtering options
    - ·Filtering by a variety of properties such as filesystem, signature, and time
    - ·Dynamic filtering operators, sorting, and grouping
    - ·Search by regular expression
    - ·Character search – Supports to search similar words
    - ·Keyword registration
    - ·Bookmarking selected data
- New digital device analysis
    - · Drone data analysis - Flight history, Multimedia data, Supports manufacturer DJI/Parrot/PixHawk
    - ·IoT device data analysis - AI Speakers, Smart TV, Car Navigation

- Python scripting IDE for user-defined analysis
  - ·Includes a Python script editor
  - · Supports generating, executing, and debugging code and includes sample scripts
- Case management and hash value verification
  - ·Various case management features
  - ·Grouping extraction images
  - ·Hash value verification on a per-image basis
- Maximized performance.
  - · High speed analysis achieved through multi-core CPU/GPU parallel processing
  - · Supports running multiple instances of the program (i.e.: one instance for each open case)
  - · Analysis status alarm – Pop-up message will let user know when forensically important data and history are found (i.e. Initialization history, Data hidden apps, Parallel space)
- Report generation
  - ·Hashing individual files
  - ·Export analyzed multimedia
  - ·Automatic report generation (PDF, Excel, HTML, XML, SQLite DB formats)
  - ·Supports 3rd party reporting formats like Nuix and Relativity
  - · Bundling feature – Bundle generated reports/outputs (exported folder, etc.) into MDF file

Technical Specifications For Social Media Darknet & Crypto

Technical Specifications for Social media investigation

- PEOPLE SEARCH: Search using just a name or a photo of the target person, find people, profiles, events, companies, and posts by geolocation, find profiles in social networks, Darknet and other resources by only nickname or alias.
- SOCIAL NETWORKS: Allows you to find the subject's profiles in all social networks and messengers simultaneously: Facebook, Instagram, LinkedIn, Twitter, Youtube, Tinder, Snapchat, TikTok, Whatsapp, Telegram, Steam, Discord and more.
- DARKNET SEARCH: Allows you to search the Darknet for closed sites without a login within more than 30 popular Darknet forums and marketplaces, search by PGP key, and archive Darknet pages
- ARTIFICIAL INTELLIGENCE methods for image and text analysis:
  - facial recognition, gun identification for photos and videos from Facebook, Instagram, YouTube and more
  - general and object sentiment analysis, topic clusterization, summarization for
- posts and texts on Facebook, LinkedIn, DarkNet and more
- CRYPTOCURRENCY AND BLOCKCHAINS: Check the cryptocurrency address for spam, retrieve address information and transfer details to analyze the flow and connect with other data points.
- Data enrichment using third-party integrations: Access PIPL, WhoisXML, Security Trails, OpenCorporates, CompaniesHouse and more
- Public Databases
- Provide 650+ search methods
- Deep Facebook search - some unique methods:
  - Get mutual friends/visited places/groups/pages/likes/comments for two Facebook users with one click.

  - If the friends list of the ‘target’ person is private, you can still get all Facebook users, who made any kind of activity with the target – likes, comments, reposts, etc.
- AI-Powered Facial Recognition - with one click, you can check the 'target' person profiles in all socials. You need only a name and a photo. Or look for the ‘target’ person in the photos on the other person’s profile, as well as in the photos from the chosen geolocation.
- Search by Geo -to search social media content. For DarkNet traffic analysis option
- Darknet search - unique search in 30+ Darknet forums and marketplaces without authorization by Phrase, PGP Key, Alias, also, you can get analytics by Products and Locations (shipping from/to).
  - Images from DarkNet searching (products, etc.).
  - Available to save web-archives for DarkNet web pages.
  - Checking EXIF data for Images (all images).
- Public databases – 9 billion records about people, companies, places and their connections. Most of the data is obtained by parsing a variety of white and yellow pages, company registers, business directories, social networks and other open online sources.
- Integration with 3rd party services via API - increase investigation efficiency to get in one workplace powerful instruments, such as PIPL, Securitytrails, Censys, ZoomEye, WhoisXML, OpenCorporates, CompaniesHouse and others.
- Advanced search - advanced searching in: Facebook, Twitter, OK, Google, LinkedIn by specific parameters. Match criteria for exact searching in PIPL and full json file with all historical records provided by PIPL.
- Search by date. Available many methods for searching by date:
  - Facebook - Photos/Videos/Posts by type All/Liked/Tagged in/Commented.
  - Twitter - using advanced Twitter search
  - Instagram - search ‘target’ person’s faces in a selected location photos by date
- Look for alias in 500+ sources. Search for user profiles with the chosen alias in more than 500 sources with one method.
- Visualization tool, additional analytics tool of collected data and built-in presentation mode with an autoplay function as well as a report building and export functionality.
- Installed on the server where the solution is deployed.
  - Users can connect directly from their devices under their
  - login and password via a secure connection through a browser.
  - To start an investigation, the user just needs to enter: text (txt, doc),
  - image (jpg, png), table (xls, xlsx) , map (kml, kmz) file , aliases,
  - phone number,email,crypto addresses .
- Graph view (with objects as labeled icons, and connections as lines, e.g. social network graph, company affiliation graph, etc.)
- Table view (objects and connections visualized as rows and their properties as columns, e.g. call detail records, suspects lists, etc.)
- Map view (points, routes and areas, e.g. cadastre, addresses, movement patterns, etc.)
- Text view (texts in general, e.g. social network posts, news articles, etc.)
- Image view (images, e.g. photos)
- View information
  - Add information (manually and automatically in the Gather phase)
  - Use information as input to the data collection algorithms (in the Gather phase)
  - Edit information (delete, append or change in the Analysis phase)

- Search and filtering within the project
- Timeline visualization for the timestamped objects and connections
- Automated machine-learning algorithms
- Natural language processing (named entity recognition, sentiment analysis,
- translation, hate speech detection, etc.)
- Computer vision (facial detection and recognition, object detection (cars, guns, etc.), etc.)
- Task manager functionality (displaying all running tasks within the project, capability to restart or stop them and view results for each task)
- Automated gathering and data processing methods run via script automation (with the possibility to create scripts with a no-code visual editor)
- Delayed, scheduled and periodical gathering and data processing methods run via monitoring functionality (with the possibility to compare results and alert users on their change)
- Social media - Facebook, Instagram, LinkedIn, Twitter, TikTok, SnapChat,
    - S,Xing, Foursquare, Blogger, VK, OK, , Tumblr, Gravatar,
    - Flickr, Github, MyMail,MySpace, Sqoop, Youtube, Steam and others
    - 500+ sources for alias-profile matching
- Messengers - Discord, WhatsApp,Telegram, Skype
- DarkNet - 30+ forums and marketplaces without authorization
- Corporate - CompaniesHouse, Companies OC, Google Companies, OCCRP, Offshores
- API integration with 3rd party services - Pipl, Bitcoinwhoswho, SecurityTrails, Censys, Shodan, ZoomEye, WhoisXML, FullContact, BitQuery, Rosette, and others
- Public Databases - 10+ TB with e-mails, aliases, names, phone numbers
- Cryptocurrency - Ethereum platform analysis, Bitcoinwhoswho
- Some more sources - Tinder, DocumentCloud, Torrents, Wikileaks, Vulners
- Search Person by Email, Name, or Phone Number
- Start with e-mail/name/phone number only and use search methods in
- combination with 3rd party services Pipl, etc. to get social media footprint
- Look for Person Using a Photo with Facial Recognition
- Having just a name and a photo, get a user's account in one click in different social networks (Facebook, Instagram,
- Linkedin, TikTok, Twitter, VK, OK, etc.)
- Or find all the target person's photos on the other person's profile.
- Complete Online Presence
- Uncover and match information about
- specific individuals in a broad range of social media and web resources
- Find Social Media Content by Geolocation
- Search photo or video content, social media pages and
- places by geo-coordinates.
- Map Crime Group Structure and Affiliation
- Analyse internal and external links between people, events, companies.
- Visualization helps to identify core elements inside the group.
- Search in DarkNet Forums & Marketplaces
- Without authorization. By Phrase, PGP Key, alias, or location

Technical Specifications for OSINT On Premise

- Ability to analyze real-world relationships between information that is publically accessible on the Internet. This includes footprinting Internet infrastructure as well as gathering information about the people and organisation who own it.
- used to determine the relationships between the following entities People.
  - Names.
  - Email addresses.
  - Aliases.
  - Groups of people (social networks).
  - Companies.
  - Organizations.
  - Web sites.
  - Internet infrastructure such as:
  - Domains.
  - DNS names.
  - Netblocks.
  - IP addresses.
  - Affiliations.
  - Documents and files.
- wide range of graphical layouts that allow for clustering of information which makes seeing relationships instant and accurate – this makes it possible to see hidden connections even if they are three or four degrees of separation apart.
- The ability to perform link analysis on up to 1 000 000 entities on a single graph.
- The capability to return up to 10 000 entities per transform.
- Includes collection nodes which automatically group entities together with common features allowing you to see passed the noise and find the key relationships you are looking for.
- Includes the ability to share graphs in real-time with multiple analysts in a single session.
- can be used for the information gathering phase of all security related work

Forensic Offline Darknet Investigation

- Should be offline darknet investigation on premises.
- should have a minimum of 32 core CPU or more.
- Should have minimum 512 GB RAM
- Should have minimum 13TB SSD configured in RAID 10
- Should have Tor hidden services. The DarkCloud Darknet dataset, with
- millions of pages from the Tor hidden services, and updated daily, will get you instantly tapped in and deliver the opportunity to learn, prevent, detect and investigate.
- should have search on Darknet Markets where Darknet trades take place on the Darknet Markets. By hooking into the DarkCloud Darknet Markets dataset, you are kept up to date on all activity in these environments within a single place.
- Should have Darknet search engine includes the secure browser based user interface offers a full featured Darknet search engine, including advanced query features, categorization, filtering and drill downs, dashboards and visual navigation.
- Product should carry 1 Years On-Site Warranty. Any Software/ Firmware updates to be provided during the Warranty Period.

- Should have ability to analyse online content offline
- should have ablity to use up to 20 examiners at the same time
- Should have Notifications, alarms, insights, full text and keywords search, data snapshots, API access
- Should carry 1 year hardware warranty and software support

Crypto Analysis

- Product should be designed as a data visualization platform for investigators conducting exploratory and investigative analysis within supported blockchains.
- Tools should have a feature where users can monitor a selection of addresses (monitoring clusters, wallets and entities is in QA) against different rules. The rule engine allows substantial level of customization. Users can choose to receive notifications via the web app, email, or API.
- Should have the Custom Risk Profile module to allow the user to customize the different parameters of the risk scores to suit their risk tolerance.
- The block explorers to allow a user to search for a block or its associated addresses and transactions. It is similar to publicly available block explorers except that it comes with additional filtering, searching, and investigative capabilities. It is also tightly integrated with other tools within our compliance suite.
- Should allow users to contribute to enriching our data set labelling by providing with entity (who controls) and flag (type of behavior) information about specific addresses. Labeling can be done via the web or an easy-to-implement API
- Should support (Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Bitcoin SV, Ripple, Stellar Lumens, Syscoin, Doge, Dash, Zcash, Cardano, Stacks, TRON and XDC Network) blockchains and their tokens
- Should have a provision to support BNB Smart Chain (BSC), Ethereum Classic (ETC), and Polygon (MATIC)
- Should have access available through login to the OEM Portal.
- Should have the exploratory graph provides an easy-to-use visualization engine with tools meant to quickly explore a large amount of blockchain data and easily follow the flow of funds.
- Should have the investigative graph provides a different workflow compared to the eGraph along with unique features like multi-chain graphing and custom clustering, allowing you to group addresses or transactions together within your own instance to increase the speed and ease the conducted investigations.
- Should have Wallet Attribution: Addresses belonging to or believed to belong to a specific entity are used to identify clusters / Wallets using established and proprietary heuristics.
- Should have Entity clustering: Labeling of addresses that are believed to belong to entities holding cryptocurrency addresses and wallets, such as Darknet Markets, VASP, and other institutions.
- Should have Automated transaction mapping: Within the eGraph options are provided for ‘auto peeling’, ‘find entity’, and ‘follow money forward’ which will automatically trace transactions forward.
- Should have Advanced filtering: Advanced filtering tools are available in both the eGraph and iGraph to quickly narrow down transactions that are relevant to your situation. These advanced filters enable you to quickly locate transactions involving entities and flags, as well as transactions occurring at certain times and containing specific values.

- Should have Block explorer: Just like a public explorer software has a built-in block explorer that updates transactions in real time. On top of the transaction information. Should provide enhanced filtering capabilities to identify addresses and transactions that meet certain criteria. When viewing the block explorer software overlays any attribution data alongside the address and transaction risk scores.
- Should have Wallet De-clustering: Allows for the de-clustering of a wallet in the visualization tool to see individual addresses. The user can combine and uncombine the cluster for individual exploration.
- Should have Color Schemes: The user can select different colors for each address of interest for easy identification.
- Should have Graph Annotation: Allows for notes to be added to the graphing screen.
- Should allow the user to monitor the group individually or collectively. For example, an exchange may wish to monitor their overall exposure as well as the exposure of their individual customers.
- Should allow users to ignore value transfers between addresses within the same group. In most cases, transfers between addresses within the same exchange do not present a risk.
- Should be able to monitor for (a) any transaction involving a watched address, (b) a per-transaction basis and be notified when the value exceeds a predefined threshold, (c) a period of multiple days - up to 90 days. This allows the user to identify many transfers occurring over a specified period.
- Should allow users to detect funds sent to or received from high-risk addresses. The level of risk is defined by the user.
- Users should be able to create any number of groups with different alert profile and can make these private, semi-private or public to all members of the organization.
- Should be able to have Primary Business Activity: This parameter is used to score an entity's primary cryptocurrency business activities.
- should be able to have Other Cryptocurrency Business Activity: This parameter is used to score an entity's secondary cryptocurrency business activities.
- Should be able to have Potentially High-Risk Activities: This parameter assesses if the entity is involved in any other high-risk activity apart from dealing with cryptocurrency.
- should have Entity Status: This Parameter scores entities according to their operational status.
- should have Registration Status: This Parameter assesses whether entities are incorporated/registered with the appropriate body in a jurisdiction.
- should have VASP Licensing Status: This parameter assesses if the entities have obtained the relevant virtual asset service provider license with the appropriate body in their jurisdiction.
- should have identified KYC/AML Policy: This Parameter assesses if entities have an identifiable KYC/AML policy
- should have KYC Implemented: This parameter assesses if entities require their users to go through a KYC verification process at any stage of their interaction with the business.
- should have Proof Of Reserve: This parameter awards entities for displaying transparency in the handling of their user's funds by conducting some form of proof of reserve validation.
- should have Required Encrypted Communication: This parameter assesses if entities require their users to use modes of encryption while communicating with them. This

requirement would entail that law enforcement wouldn't be able to access the communication between the business and its clients.

- should have Reputational Risk: This parameter assesses the adverse media coverage surrounding the entities in question.
- should have Country Risk: This parameter categorizes jurisdictions according to their money laundering risk based on various metrics.
- should have Sanctions: This parameter assesses if relevant sanctions are placed on the entities or any of their jurisdiction of operations. By default, countries sanctioned by the OFAC, EU, UN and Canada are selected. You can deselect any of these sanctions and select the sanctions that are relevant to you.
- Should have Regulatory Action Taken Against the Entity: This parameter assesses whether entities have been penalized by a regulatory authority.
- Should have Extremist Group: This parameter assesses if entities have been identified as extremist groups.
- Should have Dark Market/Web: This parameter assesses if entities sell goods or services on a darknet market.
- Should have Identified As Crime: This parameter assesses if entities have been involved in any of the following crimes.
- Should have Terrorism: This parameter assesses if entities have been involved in activities associated with terrorism.
- Should have Abuse Report: Entities or addresses that have been credibly reported for cryptocurrency abuse
- Should have Compromised Wallet: Cryptocurrency wallets whose private keys have been compromised.

Technical Specifications for Audio, Video (analysis, recognition etc.)

Video Forensic Solution

Import Capabilities

- Import video, image and audio files quickly and easily
- Batch import video sequences from VMSes like Milestone and numerous directly supported proprietary files
- Supports and manages ingest of data from multiple storage sources and device type
- Import of digital video file format, Rapidly decode video using a unique combination of Windows codecs
- Import via screen capture from proprietary player using designed capture tool
- Support advanced importation of files from Ovation systems, Timespace and others.
- Gather screen capture technical information on frames rate etc when screen capturing
- Import from analog video sources
- Import for IP network camera and over the internet
- Automatic identification of video file format for standard file types
- Player Manager solution aims to identify correct Player to play a video file
- Player Manger provides a broad range of players and information on those players
- Store proprietary players in a library, enabling you to access the right player for a video
- Ensure you can play a video by using unique library of over 800 players
- Eliminate the installation of players by using virtualized players
- Automatically analysis codec and encoding of a file type
- Import multiple different sources of video simultaneously
- Organize and display multiple sources of video relating to your case

- Add evidential metadata to you video like source, exhibit reference etc
- Correct time anomalies by offsetting the time to the speaking clock.
- Ability to add Metadata information such as file/data format, capture information (e.g. location, time, camera settings)
- Ensure the integrity of your data by using frame by frame hashing
- Deinterlace video

Viewing/Exploration Capabilities

- Display and view video on timeline
- Ability to split multiplexed video into different channels.
- Jump from one video to another video in your case quickly and easily
- Quickly review the timeline to see all motion events
- Search your video by time
- Review key events frame by frame
- Play/ Pause / Stop / Rewind video
- Speed up video playback for rapid reviewing
- Connect to jogg shuttler control device for fast review
- Pop out a video timeline to a second screen
- Rotate your video view
- Zoom in on key areas of the video to see objects clearer
- Lock timelines to view overlaps between to videos
- Ensure collaboration during a case with simultaneous multi-user access

Searching Video

- Detect moving objects in video
- Process and search video with very low frame rates
- Process video with low light and poor quality
- Filter video for objects/movement (Allows user to select/omit data for viewing based on specified criteria) by:
- Search video automatically by direction i.e. movement right, left, straight etc
- Search video automatically by object colours
- Search video automatically by region i.e. partial view of recording
- Object tracking (following of a person/object/vehicle within a video without leaving the field of view)

Report

- Create video and image reports
- Export multiple video frames to pdf document
- Add text notes to images
- Export video as a sequence of frames
- Select clips from a video manually
- Slect clips from a video by slecting all events
- Ability to export all frames in a video clip
- Ability to storyboard clips from multiple video sources (Produces a shortened video that conveys all activity from a longer video stream)
- Ability to combine videos of different frame rates and aspect ratios to the same video report
- Correctly represent all original frame rates and frame sizes
- Edit a clip frame by frame
- Add text notes to images
- Add presentation slide with fade and cross fade options
- Export to .avi/ DVD

- Save a reporting project so you can return to it at a later date
- Quickly redact or highlight key persons or events of interest using blurring, pixilation, spotlight and arrows without having to do it frame by frame.
- Suspect tagging: Functionality for the manual annotation of content, e.g. persons wearing backpacks, license plate locations, pedestrian silhouettes
- Selection and filtering of tagging by object, key word and notes
- Image & video spotlight, blur and text options
- Create interactive viewing logs of key persons of interest across video sources in your case
- Export your viewing log to excel, MS Word or PDF
- Export your viewing log and video sources to the IBM Analyst Notebook for large scale data exploitation
- All video frames individually security tagged with both an opensource and a tamper evident digital signature.
- All reports are tagged with a tamper evident digital signature

Clarification of video and images

- Clarify images and video using multiple and layer techniques
- Crop, lens distortion, perspective crop, roate image, roate or mirror, scale,
- Brightness & Contrast, contrast crop, deinterlace, gamma correction, Invert, Noise removal, sharpening, split channel, Histogram Stretch, De blur, stabilize, super resolution, temporal median
- Check data integrity with tamper evident mechanism
- Side by side viewing of 2 video streams
- Automatic speed calculation algorithm
- Export video in side by side view

Video management

- Change language
- Create named user logins and passwords
- Customized settings in Admin configuration e.g. user access, compression, reports templates
- Automatic speed calculation algorithm
- Export video in side by side view

Voice Inspector

- Adaptive Voice Comparison
- Whether you need to verify a pair of voice recordings against each other (1:1 identification) or search for a speaker within multiple audio files (1:N identification), Phonexia Voice Inspector allows you to do both so that you can choose the right approach necessary for your case.
- Automated Unbiased Analysis
- Reinforce your forensic claim with an objective voice analysis done in Phonexia Voice Inspector natively using Phonexia Deep Embeddings™—the latest generation of automatic speaker identification technology powered by deep neural networks to provide high accuracy.
- Wave Editor
- Cut through the noise quickly with Phonexia Voice Inspector's Wave Editor, which lets you automatically detect the audio parts containing speech, flag the recordings unsuitable for voice analysis due to their noise level, display a spectrogram for more detailed analysis, and much more.
- Language Independent
- Compare voice recordings regardless of their language and eliminate the need to hire a dedicated linguist specialized in a particular language as Phonexia Voice Inspector can identify the speaker's unique voiceprint in any language, making forensic analysis more efficient.
- Multiple File Search

- Analyze large amounts of audio recordings with ease using Phonexia Voice Inspector's built-in ability to search for identical phoneme sequences across multiple voice recordings so that you can work more effectively and provide forensic voice analysis on time.
- Easy Case Management
- Stay on top of every forensic case with straightforward management of audio files, population sets, and corresponding notes so that you can progress through each investigation systematically and with confidence that all case-relevant files are always in one place ready for analysis.

Voice Biomatrix

- Language Independency
- Human voice properties are so unique that even when someone tries to speak in a different language or accent, Voice Biometrics can recognize the speaker anyway.
- Channel Independency
- Whether the source of the voice comes from a phone call, YouTube video, or any other channel, Phonexia Voice Biometrics can always identify the speaker with high accuracy.
- Fast Voice Enrolments
- The latest generation of Phonexia Voice Biometrics can perform voice enrolments (the creation of a voiceprint—a digital representation of a person's voice) in as few as 20 seconds and then verify the speaker instantly with a recording only a few seconds long.
- Text Independency
- There is no need to say a specific sentence or word to be successfully recognized by Phonexia Voice Biometrics as the engine identifies speakers automatically based on their natural speech.
- Gender Identification
- By analyzing the particular acoustic characteristics of a person's voice, Phonexia Voice Biometrics can estimate the gender of a speaker with high probability.

CCTV Pro

- SEAMLESS IMPORT/EXPORT
  - Import everything from CCTV to native forensic image formats and start analyzing them straightaway.
- ADVANCED ANALYSIS
  - Bring critical clues to the surface faster with analysis algorithms for filtering, sorting and searching.
- ROBUST IMAGE AND VIDEO HASHING
  - Save valuable time and energy by pre-categorizing known data and stacking duplicates.
- GROUP AND SEARCH METADATA
  - Leap ahead in your analysis by correlating metadata to open sources on the internet.
- CUSTOMIZED REPORTING
  - Cut down on your admin work with handy functions for detailed and fully customized reporting.
- OPEN API
  - Use the third-party apps you need to crack the case thanks to the ability to add plug-ins through the API.
- GRIFFEYE BRAIN CSA (AI)
  - Automatically classify child sexual abuse content with outstanding accuracy.
- GRIFFEYE BRAIN OBJECTS (AI)
  - Automatically label image content based on thousands of concepts.
- FACE RECOGNITION
  - Detect and recognize faces in image and video using technology applied to mass volume and "real world" imagery.

Video Analytics & Forensic

- Face detection
  - find the position and location of faces in photos or videos. This usually works despite of unfavorable lighting, rotations, partial occlusion or poor video quality. In video, faces are tracked from frame to frame to form continuous tracks. These tracks can be used for more precise identification than single frames alone.
- Age and gender
  - In addition to classic identification, the age and gender of individuals can also be estimated by analyzing the face. Thus, you can create statistics on the age and gender distribution of customer groups or start searches for these features ("soft biometrics").
- Person and object recognition
  - Here people are recognized as a whole. This way, a person can be detected even if they are only partially in the picture or visible from behind only. With object recognition, you can quickly find different types of vehicles and luggage in the image and video material.
- Face recognition
  - For facial recognition, so-called templates are extracted, which represent the individual characteristics of each face in a compact way. These templates can then be compared with reference templates of query identities. Creating identities from more than one reference template ("enrollment") leads to better recognition rates than with single template comparison.
- Advanced facial features
  - You can also search for attributes such as glasses, masks, hats, beards, etc. It enables you to find people based on descriptions or, for example, to check whether or not they are wearing a mask.
- Analyze videos and photos
  - automatically locates faces and creates templates. Each face or track becomes a discoverable event.
- Live analysis
  - Cameras can be directly connected and analyzed in real time. In the live display, the resulting events can be observed as they are produced, hits are highlighted.
- Integrated video player
  - In the built-in video player, every face is "clickable". There are also comfort functions such as magnification, variable speed, brightness adjustment, multi-monitor setup, etc.
- Retrospective search
  - Using retrospective search, videos, pictures and camera recordings can be searched for identities that were not known at the time of the recording. Various sortings and filters are available. Freshly discovered sightings of a person can be added easily to the query identity in order to iteratively refine the search.
- Manage identities
  - Identities can be created and dynamically extended with events from video or image sources. Image uploads can also be used to create identities.

Technical Specifications for Advance Recovery Lab

ChipOff Lab

- FLASH READER, SOFTWARE AND READER ADAPTERS WITH SOCKETS

    - Automatic analysis functions such as XOR auto analysis, Spare area analysis, FAT/NTFS metadata analysis
    - Advanced Hex and Bitmap viewer
    - Scramble extractor (XOR key)
    - Automatic ECC detection and virtual image correction
    - SQL database of NAND chips and controllers
- Supported NAND packages: TSOP48, LGA52, LGA60, TSOP56, BGA100, BGA152, BGA154, BGA224
- MONOLITHIC ADAPTERS FOR FALSH READER
- Full set of adapters with socket to read FLASH monolithic devices such as MicroSD and USB thumb drives without the need of soldering wires to a standard TSOP adapter Monolithic chips Samsung, SanDisk, Hynix, Toshiba, Intel, Micron and others
- EAGLE BUNDLE
- Hardware and software complex capable to acquire and extract data from:
    - Fully working and unlocked devices
    - Locked and/or damaged smartphones and tablets (chip-off)
- Read and extract data directly from the memory chips through chip-off
- COLD CHIP-OFF
    - An automatic engraver to perform chip-off, even though it doesn't fully replace traditional hot procedure
    - Controlled remotely thourgh a tablet (included) and wifi direct connection.
- JTAG/ISP TABLE
    - Used to connect the TAPs of Jtag interface or ISP without the need of soldering wires
    - Non destructive way to read memory chip content for older phone with active Jtag interface or known ISP pinout

Technical Specifications for Drone Forensics

Drone Forensic

- Various extraction methods for wide range of drone aircraft

  - Extraction through the drone aircraft USB connection

  - Extraction through the network connection (WiFi)

  - Extraction through SD card

  - Chip-off Extraction (Requires memory Chip socket and reader)

  - drone App data can be extracted with MD-NEXT and exported with MD-RED

  - Provides an Extraction guide for each method

- Timeline-based integrated flight data analysis

  - Timeline-based flight parameter values (speed, altitude, value of each motor, etc.) can be viewed in graphic format

  - Drone's position and posture (Yaw, Roll, Pitch) information on the timeline

  - Integrated view of flight history and media data preview on the Timeline

  - Playback and reconstruct flight history on the map

- Check the selected media in the Timeline chart

- Deep analysis of flight data by AI and machine learning

  - Learning of accidental or abnormal filight log data

  - Find out the collision, battery exhaustion, normal landing and abnormal filight position/time

  Detail flight data view and selection

  - Detailed values of the flight log in the table and visualization on the map

  - Classify meaningful flight log values such as altitude, ground speed, battery, and signal strength and display in different colors on the map

  - table view of GPS-based drone track, latitude, longitude and movement history

  - Sorting and filter flight data in time order

- Multimedia gallery

  - Select the multimedia (video, photo) file with the matching time information in the flight record

  - filter the multimedia file by such as the path, creation date, and size

  - Intuitive analysis through the preview feature

- Bookmark

  - Supports bookmark feature for flight time range, image and video

- Notification

  - Displays and saves important notifications during Extraction and analysis while using the product in the notification center

  Report generation

  - Supports to export reports in PDF format based on the bookmarked contents

  - Supports to export each manufacturer's flight log glossary in csv format

  Multimedia Export

  - Supports to export the acquired original multimedia data (photo, video)

- Supported drone aircraft list - aircraft - USB connection

• DJI (Phantom 4 series, Mavic Pro series, Inspire 2, Matrice 600), • Yuneec Typhoon H Plus, • ALLNEWTECH ANT-H5, • Sundori SDR-H-2021, SDR-M1, • EFT (EFT-E610, Flight Control Computer - USB connection, • DJI (A3, N3), • PixHawk (PixHawk4, The Cube, V5+, PX4_2.4.6, PixHawk New X7, PixHawk V5+, PixHwak2 Cube Orange, SD Card of Drone), • DJI (Phantom 3, 4 series, Mavic Pro series), • PixHawk (PixHwak4 series, PX4 2.4.6 series, Cube, V5+, X7), • Yuneec Typhoon H Plus, • All UAVs which use SD Card for their multimedia storage Chip-off, • DJI (Mavic 2 Pro, Mavic Air, Mavic Air 2, Spark, FPV, Matric 300), • Parrot (Bebop2, WiFi Network), • Parrot Bebop2

Technical Specifications for On-scene Forensics

forensic FlyAway Kit with Field Triage and Ballistic Imager

- Must be designed for Mobile IT Forensics Analysis on the Field
- should have the all accessories include all Tableau writeblockers and sufficient destination drives to image every medium found out in the field.
- Should have all the Adaptors and bridges like SATA/IDE Bridge, SAS Bridge, PCIE Bridge, USB Bridge, Firewire Bridge including :
    - Multipack Harddisk Adapter Set
    - UltraBlock USB 3.0 Forensic Card Reader
    - 2x Hard drives cooler IceBay
    - Multi-Card-Reader USB 3.0 incl. 2x Micro SD/SDXC-Adapter to SD and 2x Mini SD Adapter to SD
    - Active USB 3.0 Hub
    - ExpressCard/34, FireWire 800 (IEEE 1394b)
    - Thunderbolt to FireWire Adapter
    - USB to Lightning Cable
    - Thunderbolt Cable ST/ST
    - Adapter DisplayPortST to DVI BU 15cm
    - USB 2.0 Cable A/Micro-B
    - USB 3.0 A/Micro-B
    - USB 3.0 Cable A/B
    - Cable USB 3.0 Y 1xUSB 3.0 micro
    - USB 2.0 Y Cable 2x Typ A to Mini B
    - USB 3.0 Adapter cable, Typ-A/Typ-B
    - Adapter eSATA-socket zu SATAStecker
    - Interfaces converter M.2 NGFF, SATA
    - USB 3.1 Cable Typ C/Typ A
- Portable rugged forensic laptop system
    - Display: 17,3“, non-reflective (1920x1080)
    - Processor: Intel i7-8700K 4,7 Ghz Processor
    - RAM: 64 GB
    - Video Card: NVIDIA GeForce GTX1080 8GB
    - System: 512 GB SSD, M,2 NVMe PCIe x4 2x 2 TB SSD SATA III
    - Optical Drive: Blue-ray RW
    - Communication: WIFI+Bluetooth 1 Gigabit LAN RJ-45
    - Battery: 8-cells smart li-ion
    - Keyboard: with backlight
    - Security: Integrated fingerprint scanner, TPM 2.0 security chip
    - Connections: 2x USB 3.1 type C / Thunderbolt 3 / DP 1.3 / HDMI 2.0, 4x USB 3.0 (1x USB powered), 2x miniDP 1.3, 1x HDMI 2.0 output, 1 x 2-in-1 audio jack, (headphone / S/PDIF optical output), 1 x microphone-in, 1 x line-out, 1 x line-in, 1 x RJ-45 LAN, 1 x DC-in
    - Software: Windows 64 bit (8.1 / 10), optional Linux 64 bit
    - Forensic Imaging Tools: AccessData FTK-Imager, Tableau Imager, Computer Imager, Guymager (Linux)
- Should have 12 Months Warranty
- Should be able to achieve blisteringly-fast acquisition times using the subject machine to image itself out.
- Should be able to split the imaging process to multiple collectors; utilising all available ports, either in a ‘live’ state or boot mode.
- Should be able to work on Windows, Mac and Linux.
- Should have an ability of forensically sound, with MD5, SHA1 & SHA256 validation.

- Should be able to stop extractions before completion without the risk of losing any data acquired up to that point.
- Should allow recovery of deleted data.
- Should have funcuotn of no need to remove the hard drive.
- should have Rapid automated triage solution.
- Should provide alerts of suspicious items through a red, amber and green status.
- Should have abability of Highly configurable search profiles.
- Should be able to quickly acquire usernames and passwords.

Triage for Computer and Mobile

- tool to allow police to find evidence of child abuse or terrorist activity on suspect's computers in just minutes, replacing processes that take weeks or months in a forensics lab.
- Should have EXAMINER
  - More experienced/technical users
  - Used on scene and in the station
  - Fully configurable by the user
  - Some setup is required
- Should have OFFENDER MANAGER
  - Designed specifically for OM/field use
  - Used on scene
  - Configurable by the supervisor
  - No set-up by a user required
- Should have FILTER BUILDER
  - Creates a Contraband Filter Plugin from up to 10,000 files
  - Allows suspect devices to be scanned for this new material alongside the existing Contraband Filter
- Should have COLLECTOR
  - Creates a Contraband Database by extracting information from the original material
  - Process datasets of up to 100k files
- Should have RUGGED TABLET WITH PELICAN CASE
  - Intel® Core™ i5-1135G7 Processor
  - Intel® Iris® Xe Graphics
  - 11.6" IPS TFT LCD FHD (1920 x 1080)
  - AC adapter (90W, 100-240VAC, 50/60Hz)
  - Li-ion smart battery (11.4V, typical 2680mAh; min.
  - 2640mAh) x 2
  - 8GB DDR4
  - Touchscreen
  - TPM 2.0
  - Kensington lock
  - Accessories
  - Pelican case with customized foam
- Identifies previously known files, and shows their category/classification
- Detects remnants of deleted and partially downloaded files
- Detects and warns of high levels of encryption on disk
- Full control of scan options
- Results preview using forensically sound internal viewer
- Detailed results, with PDF report
- Run from a forensic computer, bootable media or live on a suspect computer
- Simple Red/Amber/Green result
- Pre-configurable by expert users
- Simple user interface

- Quickly collect up to 10,000 newly recovered files
- Scan for new material alongside an existing Contraband Filter
- Accelerate triage by finding evidence in seconds or minutes
- Target offences involving Child Sexual Abuse Material or Terrorism images
- Detects partially deleted and partially downloaded files
- Allows flexibility to create investigation-specific Contraband Filters
- Enables investigators to confirm if new material has been uploaded elsewhere
- Inherently secure
- Power tool to share and use confidential data in frontline tools
- Search speed is unaffected as the Contraband Filter size increases

Portable Write Blocker-Multi in one

- Must be very small, very light, extremely versatile, highly usable and easy to carry
- Should have Integrated Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface
- Must have Retractable Ice Tray internal cooler for suspected drive
- Must have Forensic Card Reader for Compact Flash Card (CFC) - MicroDrive (MD) - Memory Stick Card (MSC), Memory Stick Pro (MS Pro) - Smart Media Card (SMC) - xD Card (xD), Secure Digital Card (SDC and SDHC) - MultiMedia Card (MMC)
- Must have 1x 4TB Enterprise HDD, SATA III in removable tray
- Must have Trayless Mobile Rack for 3.5" SATA HDDs
- Must have 2-Port USB Read/Write port Hub
- Must have 5x Anti-Static DriveBox for 3.5" HDD's (empty)
- Must include a cable set with all the necessary connector cables, adapters, a fine tool-kit and a sturdy but lightweight case (cabin luggage size) for easy transportation.

Forensic Fast Imager

- Capable to imaging/clone data from one to one, two to two or one too many destination media
- Capable to imaging/clone data at the speeds of 50GB/min or higher. Clone PCIe to PCIe at speeds of 90GB/min
- Support multiple Imager Formats , copy, dd image,.drug image, e01, ex01, supports MD5, SHA1, SHA256 and dual-hash (MD5+SHA-1) authentication
- Should Image & verify from 5 source to 9 destination drives for ultra efficient imaging
- Multiple Imaging Ports:
- write-protected source ports include :
- 2 SAS/SATA
- USB 3.0 (can be converted to SATA using an optional USB to SATA adapter)
- PCIe
- I/O ports for use with optional I/O cards including Thunderbolt 3/USB-C
- 9 destination ports include:
- SAS/SATA
- 2 SATA only
- USB 3.0 (can be converted to SATA using an optional USB to SATA adapter)
  - PCIe
- I/O ports for use with optional
- I/O cards including Thunderbolt 3/USB-C.
- Should have Two 10GbE network ports for network connectivity. The unit should include a USB 3.0 device port for drive preview and two USB 2.0 host ports
- Should allow imaging to an external storage device such as a NAS, using the 10GbE ports, USB 3.0 or via the SAS/SATA connection.
- Should be able to Simultaneously perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Image simultaneously from multiple sources to multiple destinations including a network repository. Supports imaging to one location while

simultaneously hashing and/or wiping a second drive. Perform up to 5 tasks concurrently. Little or no speed degradation when imaging from two sources to two destinations

- Capable Web Browser/Remote Operation to allows to connect with device from a web browser
- Capable to cross copy support for IDE, SATA, e SATA, microSATA, SAS, ZIF and USB interface and combine-SATA etc.
- Should image CD/DVD/Blu-ray media by using a USB optical drive connected to the USB port on the device
- Capable to Detect and capture Host Protected Areas (HPA) and Device Configuration Overlay (DCO) hidden areas on the source (suspect) drive
- Should Capture network traffic, internet activity and VOIP.
- Capable to Generate Audit Trail Reporting/Log Files in XML, HTML or PDF format
- Should Secure sensitive evidence data with whole drive AES 256 bit encryption
- Allow to manipulate the DCO and HPA area of the destination drive so that the destination drive's total native capacity matches the source drive
- USB Host Ports and HDMI Port for connecting keyboard, Mouse and with Projector
- Forensic, Filter-Based File Copy, users can filter and then image by the file extension (such as.PDF,.xls, JPEG, .mov etc.).
- Capable to acquire data over a network
- Capable to generate the log of the processes
- Capable to boot/mount the suspect media virtually in a write protected environment for preview of live data.
- USB Host Ports and HDMI Port for connecting keyboard, Mouse and with Projector
- Product should carry 1 Years On-Site Warranty.
- Any Software/ Firmware updates to be provided during the Warranty Period.

Malware Testing Platform/Lab

Functional Specification- Malware Testing Platform/Lab Software

Realistic simulation of cyber-attacks: Digital Twin should provide a controlled environment where digital forensic analysts can simulate various types of cyber-attacks, allowing them to practice and enhance their investigation and response skills. This hands-on experience helps them develop the expertise needed to identify and analyze digital evidence in real-world scenarios.

Training and skill development: Digital Twin should offer training modules and scenarios specifically designed for digital forensic investigations. Analysts can engage in simulated investigations, learning to navigate complex network architectures, analyze logs and network traffic, and extract digital evidence. This practical training enhances their proficiency in forensic tools and techniques.

Replication of diverse cybercrime scenarios: Digital Twin should enable the replication of a wide range of cybercrime scenarios, including malware infections, network intrusions, data breaches, and insider threats. Forensic analysts can practice investigating these scenarios, gaining valuable experience in handling different types of cyber incidents.

Controlled experimentation: Digital Twin should provide a safe and controlled environment for forensic analysts to experiment with various investigative methodologies, tools, and techniques. They can explore different forensic software, test new approaches, and assess the effectiveness of different forensic strategies without compromising real-world systems or networks.

Collaboration and teamwork: Digital Twin should facilitate collaborative exercises, allowing multiple forensic analysts to work together on complex investigations. They can share information, coordinate efforts, and learn from each other's experiences. This fosters teamwork and collaboration, which are essential in real-world digital forensic lab environments.

Scenario customization: Digital Twin should be customized to replicate specific environments or industries, such as financial institutions, government networks, or industrial control systems. This allows forensic analysts to practice investigations within the context of their target sectors, gaining domain-specific knowledge and skills.

Time compression: Digital Twin should enable the acceleration of time, allowing forensic analysts to compress hours, days, or weeks of simulated activity into shorter time frames. This helps analysts quickly evaluate different investigative approaches, learn from mistakes, and improve their efficiency in handling digital evidence.

Evidence preservation and analysis: Digital Twin should provide virtualized environments where analysts can capture and preserve digital evidence without the risk of data corruption or tampering. They can perform in-depth analysis, conduct memory forensics, examine file systems, and extract artifacts while ensuring the integrity of the evidence.

Continuous learning and improvement: Digital Twin Should offer the opportunity for ongoing learning and improvement. Analysts can regularly engage in simulated investigations, keeping their skills sharp and up to date with emerging cyber threats and forensic techniques. They can also evaluate their performance, identify areas for improvement, and refine their investigative processes.

Forensic tool evaluation: Digital Twin should serve as a platform for testing and evaluating new forensic tools and technologies. Analysts can assess the effectiveness and reliability of different software, hardware, or methodologies in a controlled environment before deploying them in actual forensic investigations. This helps ensure that the tools used in the digital forensic lab are efficient and accurate.

Technical Specification -Malware Testing Platform/Lab Software

- The proposed solution should provide extensive training programs and comprehensive documentation to enable users to effectively utilize the forensic lab solution.
- The solution should offer hands-on training sessions covering the proper handling of digital evidence, forensic analysis techniques, and the utilization of the supported forensic tools.
- "The proposed solution must allow participants to perform following ,but not limited to, cyber forensic activity.
    1. Network Forensic
    2. Malware Forensic
    3. Email Forensic
    4. Mobile Forensic
- Comprehensive documentation should be provided, including user manuals, guides, and reference materials that outline the functionalities and best practices of the forensic lab solution.
- The proposed solution must allow participants to capture network packets in real time and analyze the captured packets for any malware related activity.
- The proposed solution must allow participants the acquisition and analysis of data from various sources, including hard drives, network traffic, and mobile devices**.**
- Solution must offer a comprehensive suite of forensic tools to facilitate evidence analysis and examination. List of supported tools - EnCase, FTK, Autopsy, Volatility, and Sleuth Kit."
- The solution must support Evidence Acquisition activity:
    - Support reliable and forensically sound acquisition of digital evidence from diverse sources.
    - Include capabilities for disk imaging, file system extraction, memory dump analysis, and network traffic capture.
    - Ensure data integrity and chain of custody throughout the acquisition process."

- The solution must offer single forensic lab or a mix of multiple forensic labs to be executed at the same time. For example, to replicate a scenario where there is network attack along with malware spread through email misconfiguration. So when the lab is run all three situations must run in parallel to demonstrate real world learning capability.
- The training and documentation should cater to users with varying levels of expertise, ranging from beginners to advanced forensic analysts.
- Continuous support and updates should be available to address any questions, concerns, or emerging trends in the field of cyber forensics

- Proposed Solution should be able to deploy on-premises and in the cloud.
- The Proposed Solution should be able to run the not blocked and not detected attack on the test range for Blue teams to learn about Specific mitigations and there effect on production Systems
- The Proposed Solution should be able to recreate access flows to learn best way to deploy the mitigation recommended
- Proposed Solution should facilitate Red Team and Blue Team and Purple team tactics in a simulated lab.
- Proposed Solution should simulate the network of at least 60 real systems including the real applications, Microsoft AD environment servers, routing & switching equipment. This is required to simulate a real world data centre.
- The Proposed Solution should provide a virtualization or integration and emulation of security controls
  - Multilayer NGFW
  - Web Application Firewall
  - Network IPS
  - EDR, Host IPS & FIM
  - Network Behavior Anomaly
  - SSL Interception
  - DNS Security
  - Security Orchestration Server
  - Proposed Solution should provide a virtualization and emulation of following systems similar to Data center
    - Apache and Microsoft Web Servers
    - SQL Databases
    - Windows Desktops
    - Linux Desktops
    - Applications Server
    - Mail Server
    - Custom DNS Server
    - NMS Server

- Proposed Solution should be able help understanding any cyber breach possibility in the network and take proactive steps.
- Proposed Solution should be able help to automate responses for better Cyber Control
- Enhancing the skills of existing staff by Participating in Incident response drills
- Instructor Application: Should Allow the instructor to easily set up a training, run a training, and perform the debriefing of a training. Includes the following:
  - Real Time Monitoring
  - Candidate Evaluation
  - Candidate Progress Tracking
  - Session Recording
  - Training History
  - Training Reports

- Drill management console should provide an Intuitive graphical user interface (GUI) enabling trainers to configure and run training sessions.
- The Drill Management Console should provide option to influence the level of difficulty of the scenario and simulating more sophisticated attackers, by modifying parameters such as changing attack duration, deleting logs during the attack, and performing a silent attack.
- Proposed Solution should have inbuilt capability of MIDR, Automation tools to formulate the Threat facing configs
- Cyber Platform/Range should also be able to test Config validation for its efficiency and reliability.
- Proposed Solution should be able to Fetch mitigation and IOC information and supply the information to SOAR tools if required
- The Proposed Solution Should provide testing of mitigations and generate purple config in specific form which can be utilized by Security Controls directly.
- Solution must be supported by an in-house/ external threat intelligence group for providing threat updates on a regular basis, including features such as daily malware feeds and must also include attack Tactics, Techniques, and Procedures (TTPs) from multiple APT groups including those based on the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework.
- Solution should provide the real payload and not just IOC in threat details. Solution Should also be able to provide complete details of attack.
- Solution should have the ability to create new attacks by integrate sample collected or sourced from other platform. This should not require any OEM intervention User should be able to that by themselves.
- Solution should come with inbuilt threat builder to easily create scenarios with click of buttons.
- Solution should be able to Create dynamic attack groups so that future attacks are automatically added into the group.
- Solution should be able to provide threat payload so that in case of Zero day attack One can create there own Snort Signatures and push them in production to stop any Zero day attack.
- The Threat Repository included in the proposed solution shall receive updates on a near daily basis.
- The proposed solution should provide emerging threats without any extra licenses. If needed, extra licenses should be included in the offer.
- The proposed solution should provide ready to use static threat templates for Emerging and Suggested Threats that can also be modified by the user for customized needs.
- The proposed solution should provide ready to use dynamic threat templates for Security Posture Management such as Readiness Against Ransomwares, Readiness Against APT Groups.
- The proposed solution should provide the aforementioned dynamic templates to be customized by the user.
- The proposed solution should provide the custom creation of dynamic templates with filters such as; Threat Name, Tags, Attack Category, Threat Actors, Unified Kill chain, MITRE ATT&CK Tactics, Affected OS, Severity, and Release Date.
- The proposed solution should be able to automatically add newly added attacks to the dynamic templates without user intervention.
- The proposed solution should allow users to simulate all available attack module actions for posture visibility.
- The proposed solution should use real-world malicious attack payloads for File Download, Email, and Web Application Attacks while testing network security controls.
- Threats contained in the threat database should be referenced according to the following set of information, including but not limited to: a) Unique identification number of the threat (unique ID), b) Release date of the threat, c) text-based description of the threat, d)The severity of the threat is according to the following scale: Low, Medium, High. e)Affected Platforms, f) Targeted Sector, g) Targeted Region h) Attacker's Objectives, I) Actions, j) Payloads, Executed Process Command Lines or Hash Values based on Attack Type, k) References in publicly known databases: virus total, l)References in the following industry-

recognized threat scoring and enumeration systems: CVE, CWE, CVSS, OWASP. m) Operating systems affected by the threat

- The proposed solution should allow users to create custom Windows Endpoint Scenario attacks using MITRE ATT&CK framework
- The proposed solution should allow users to create custom Network Infiltration (File Download) attacks, custom Web Application attacks with malicious payload, custom Web Application payloads, Email attacks using existing threat Repository
- The proposed solution should allow users to upload their custom attacks ,Malicious Codes or Vulnerability Exploits payloads, Hashes etc to the Threat Repository for for web application attack, email attack, network infiltration attacks, End Point attacks and data exfiltration attack
- The proposed solution should allow users to add Play and Rewind processes with the following information to be added: a)Path and Argument, b)Ability to Add a Remote File, c) Ability to Use a Local File, d)Define Result Logic, e)Metadata Information f)Action Details
- The proposed solution should be able to move laterally to achieve a defined object by the admin. The proposed solution must not require an agent to do the validation.
- The proposed solution should allow users to initiate the actions with following binary executables: a)Execution via New Threat Creation b) Execution via APC Injection, c)Execution via Call-Back
- The proposed solution should have the following attack methods in this module: a)Lateral Movement b)Kerberoasting c)Local Privilege Escalation d)Harvesting and Spreading Actions
- The proposed solution should have the following harvesting actions available: a) Local Service Misconfiguration Enumeration, b)Remote Management Users' Enumeration, c)Session Enumeration, d) LSASS Credential Dumping, e) Domain Object Enumeration, f)Domain DNS Enumeration, g) Organization Units Enumeration, h) Domain Trusts Enumeration, i)Domain Service Account Enumeration, j)Remote Desktop Users' Enumeration, k)Distributed COM Users Enumeration l)Local Admin Enumeration,
- The proposed solution should have the following access actions available: a) Windows Management Instrumentation (WMI) b) Unquoted Service Path Escalation c) Modifiable Service Escalation d) Modifiable Service Binary Escalation e) Server Message Block Execution (SMBExec) f) Pass the Ticket g) Bypass UAC via Fodhelper
- The proposed solution should have the capability to evade its operations from security controls.
- The proposed solution should have the capability to export lateral movement findings as a CSV report with following information: a) Discovered Hosts (IP and Name), b)Discovered AD Group DNS c) Discovered Domain Users (Username and Password)
- The proposed solution should map the movement of the simulation in the GUI.
- The proposed solution's attack database should include at least 1900 (one thousand and nine hundred) network infiltration (file download) threats in the threat library.
- The proposed solution should allow users to create custom: a) Windows Endpoint Scenario attacks using MITRE ATT&CK framework action library with at least 1000(one thousand) Endpoint Scenario Actions available. b) Network Infiltration (File Download) attacks using existing threat library with at least 8000(eight thousand) malicious files available.
  c) Web Application attacks using existing threat library with at least 2000(two thousand) malicious payloads available. d) Email attacks using existing threat library with at least 7400(seven thousand and four hundred) malicious files available.
  e) Data Exfiltration samples using the existing threat library with at least 200 (two hundred) sample files available. f) Vendor should be able to sign SLA of 24 hrs for adding any global critical attack in a threat library
- The Proposed Solution should be able to provide in built Threat campaign like Emerging threats, Top 10 ATT&CK techniques, Top 10 Ransomware attacks, Top Vulnerabilities exploited by State actors etc.

- The Proposed Solution should be able to create a test range with Specific Cyber Security Technology like in Data centre which should be close replica of customer specific environment
- The Proposed Solution should be able to run the not blocked and not detected attack on the test range for Blue teams to learn about Specific mitigations and there effect on production Systems
- The Proposed Solution should be able to recreate access flows to learn best way to deploy the mitigation recommended

- Proposed Solution should facilitate Red Team and Blue Team and Purple team tactics in a simulated lab.
- Proposed Solution should be able to deploy on-premises and in the cloud
- Proposed Solution should simulate the network of at least 60 real systems including the real applications, Microsoft AD environment servers, routing & switching equipment. This is required to simulate a real world data centre.
- The Proposed Solution should provide a virtualization or integration and emulation of security controls
  • Multilayer NGFW
  • Web Application Firewall
  • Network IPS
  • EDR, Host IPS & FIM
  • Network Behaviour Anomaly
  • SSL Interception
  • DNS Security
  • Security Orchestration Server
- Proposed Solution should provide a virtualization and emulation of following systems similar to Bank
  • Apache and Microsoft Web Servers
  • SQL Databases
  • Windows Desktops
  • Linux Desktops
  • Applications Server
  • Mail Server
  • Internal DNS Server
  • NMS Server
- The platform should have automatic traffic generator built in. The start stop time should have historical elements such that the trainee is not able to easily detect start of event
- Proposed Solution should be able help understanding any cyber breach possibility in the network and take proactive steps
- Proposed Solution should be able help to customize Cyber Security solution as per specific needs of organizations
- Proposed Solution should be able help to automate responses for better Cyber Control
- Enhancing the skills of existing staff by Participating in Incident response drills
- While performing training exercises for the User SOC team using this tool, then each participant should be assigned a designated role, for e.g. SOC analyst, firewall administrator, EDR Admin. The roles should be displayed throughout the exercise so as to provide better visibility of learning outcomes.
- User SOC team should be able to choose appropriate Role based access to the tool such that they can chose between a simulation exercise or a learning exercise. There should be separate environment for both the use cases and historical data will be stored for minimum of six months.
- Instructor Application: Should Allow the instructor to easily set up a training, run a training, and perform the debriefing of a training. Includes the following:
  • Real Time Monitoring
  • Candidate Evaluation
  • Candidate Progress Tracking
  • Session Recording
  • Training History
  • Training Reports
- Drill management console should provide an Intuitive graphical user interface (GUI) enabling trainers to configure and run training sessions.
- The Drill Management Console should provide straightforward setup of a Drill session including student assignment, network selection, and scenario selection
- The Drill Management Console should allow tracking and grading trainee performance.
- Drill Management Console should provide the option to execute, control and monitor the flow of the session in real time.

- The Drill Management Console should provide option to influence the level of difficulty of the scenario and simulating more sophisticated attackers, by modifying parameters such as changing attack duration, deleting logs during the attack, and performing a silent attack.
- The Drill Management Console should provide a view of the training network info via the trainer and trainee interface (in a format such as JPEG, CSV etc.)
- The Drill application shall provide an indication if a goal was automatically detected\achieved by the students. The Drill manager can edit and rewrite the system feedback.
- Proposed Solution should have inbuilt capability of MIDR, Automation tools to formulate the Threat facing configs
- Cyber Range should also be able to test Config validation for its efficiency and reliability.
- Proposed Solution should be able to Create Workflow and automate the remediation by reconfiguring the device.
- Proposed Solution should be able to Fetch mitigation and IOC information and supply the information to SOAR tools if required
- Proposed Solution should be able to wite custom IPS signatures, Operationalize IOC's Like hash, Payload information in AV for all the attacks for which Signatures are not available.
- Proposed Solution Should be able to Integrate IOC from Multiple Threat feeds -Gov, OSINT, Commercial and provide the same to Create New Attacks over API
- The Proposed Solution Should provide testing of mitigations and generate purple config in specific form which can be utilized by Security Controls directly.

11 BILL OF MATERIAL

S.No.	Topic	Product	Qty
1	Central Lab Hardware	Forensic Core Server Stack	1
2		Password Acceleration Server	1
3		Forensic Integrated Workbench	10
4		Forensic High end workstation	10
5		Forensic Parellel Data Extraction - Multi channel Mobile Analyzer and Charging station	1
6	Central Lab Software	Central Lab Software	1
7	Computer Forensics	Forensic All in one for Computer + Mobile + Cloud	5
8		Evidence Center Software	5
9		Computer Forensics Software	5

10	Mobile Forensics	MOBILE DEVICE EXTRACTION All in One	5
11		Computer with Mobile forensic	5
12		Forensic 8 channel Mobile Analyzer	5
13		Chinese Phone Extractor	5
14	Social Media /Darknet / Crypto - intelligence, monitoring and Forensics	Social Media Investigation	1
15		OSINT On Premise	1
16		Forensic Offline Darknet Investigation	1
17		Crypto Analysis	1
18	Audio, Video (analysis, recognition, Authentication and Forensics)	Video Forensic Solution	1
19		Voice Inspector	1
20		Voice biomatrix	1
21		CCTV Pro	1
22		Video Analytics & Forensics	1
23	Advance recovery Lab	Chipoff Lab	1
24	Drone Forensics	Drone Forensic	1
25	Onscene Forensics	Flyaway Kit	1
26		Onscene Kit	1
27		Triage for Computer and Mobile	1
28		Portable Write Blocker multi in one	1
29		Forensic Fast Imager	1
30	Professional Service OEM	Implementation and Knowledge Transfer Training	1
31	Niche Trainings	SocialLinks	1
32		Maltego	1
33		Qlue	1
34		Video Forensic	1
35		Phonexia	1
36		Video Analytics	1
37		Chipoff Training	1

38	Expert Manpower	L1	8
39		L2	5
40		L3	4
41		PM	1
42	Cyber Validation Platform	On-Prem/Cloud Cyber Range	1

12 CONTRACT PERIOD

Then engagement of the service provider shall be for a period of 1 year from the date of commencement service i.e. dates of Go-Live.

12.1 Timeline and Penalty

12.1.1 Delivery, Installation and Commissioning

Requirement	Timeline	Penalty
Supply of material (both appliances and software licenses)	Within 20 weeks from the issue of work order	0.5% per week of delay against theun-delivered material cost
Installation and commissioning	Within 4 weeks from the date of supply of materials	0.5% per week of delay against theInstallation and Commissiong cost
Replacement of support staff	Within 1 weeks from resignation of existing support staff/instructions from OCAC on replacement of staff	1% per week against monthly manpower cost

12.1.2 Penalty for Non-Availability/Downtime of Service

Level of availability calculated on monthly basis	Penalty Amount
> 99% or more	No penalty would be deducted
>=98% and < 99%	2% of amount payable
>=96% and < 98%	5% of amount payable
>=95% and < 96%	7% of amount payable
< 95%	10% of amount payable

Penalty for non-availability/downtime of service shall be applicable on the total quarterly usage billed amount the respective quarter which the downtime has been recorded for.

12.1.3 Other Penalty terms

a. The maximum total penalty in any quarter shall not be more than 10% of the total amount due for the quarter.

b. Penalty of 10% for consecutive two quarters may be treated as breach of contractand OCAC may take suitable actions accordingly.
c. Maximum penalty shall not be more than 10% of the total due.
d. Payment shall not be imposed, if the cause of delay/non delivery service is notattributable to bidder.

12.2 Payment term

12.2.1 Appliance Cost

a. 60% of the appliance cost shall be paid after delivery of the material andverification thereof.

b. 20% of the appliance cost shall be paid after Installation and commissioning.

c. Balance 20% of the appliance cost shall be paid after successful running of the appliances for a period of three months. This payment shall be made after deduction of Penalty for Non-Availability/Downtime of Service as described in clause 12.1.2, if any.

12.2.2 License Cost

100% of the license cost shall be paid after Installation and commissioning.

12.2.3 Installation and Commissioning

a. 70% of the installation and commissioning cost shall be paid after Installation and commissioning.

b. Balance 30% of the installation and commissioning shall be paid after successful running of the appliances and software for a period of three months.

12.2.4 Warranty support and subscription cost

a. 100% of the yearly cost against warranty support and subscription (as mentioned at Clause no. 11 Bill of materials) shall be released beginning of the respective year w.r.t date of commissioning.
b. This payment shall be made after deduction of Penalty for Non-Availability/Downtime of Service as described in clause 12.1.2 for the previous year, if any.

12.2.5 Support Resource cost

a. 100% of the payment towards cost of manpower resource shall be paid quarterly basis.

12.3 General Condition of Contract

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

- "Applicable Law" means the laws and any other instruments having the force of law in India.
- "Bidder" means the entity bidding for the services under the Contract.
- "Solution Provider" means M/s ____whose proposal to perform the Contract has been accepted by the Purchaser and is named as such in the Agreement and may provide or provides the Services to the Purchaser under this Contract.
- "Contract" means the Agreement entered into between the Purchaser and the Solution Provider, together with the contract documents referred to therein, including General Conditions (GC), the Special Conditions (SC), all the attachments, appendices, annexure, and all documents incorporated by reference therein.
- "Deliverables" means the services agreed to be delivered by Solution Provider in pursuance of the agreement as defined more elaborately in the RFP;
- "Effective Date" means the date on which this Contract comes into force i.e. Date of issuance of Purchase Order (referred as PO).
- "Day" means a Govt. of Odisha working day.
- "GC" mean these General Conditions of Contract.
- "Government" means the Government of Odisha
- "In writing" means communicated in written form with proof of receipt.
- "Intellectual Property Rights" means any patents, copyrights, trademarks, trade names, industrial design, trade secret, permit, service marks, brands, proprietary information, knowledge, technology, licenses, databases, software, know-how, or other form of intellectual property rights, title, benefits or interest, whether arising before or after execution of the Contract.
- "Member" means any of the entities that make up the joint venture / consortium / association, and "Members" means all these entities.
- "Man-Month" means one resource working for 1 month (Calendar working days as per Govt. of Odisha).
- "Party" means the Purchaser or the Solution Provider, as the case may be, and "Parties" means both of them.

- “Personnel” means persons hired or appointed by the Solution Provider and assigned to the performance of the Services or any part thereof
- “Purchaser” means Odisha Computer Application Centre, Designated Technical Directorate of Information Technology Department, Government of Odisha an entity purchasing the services under this Contract.
- “Resident” means normal resident of Odisha
- “RFP” means Request for Proposal invited for Selection of System Integrator for provision of Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha vide RFP Reference No.: OCAC-SEGP-INFRA-0007-2022-******.
- “SC” means the Special Conditions of Contract by which the GC may be amended or supplemented.
- “Services” means the work to be performed by the Solution Provider pursuant to this Contract, as described in Appendix-A hereto.
- The "Selected Agency" means Agency which is selected through the tender process i.e. System Integrator / Solution Provider.
- The "Service Provider (SP)" means service Provider engaged for the messaging service

12.4 Interpretation

In this Agreement, unless otherwise specified:

- References to Clauses, Sub-Clauses, Paragraphs, Schedules and Annexures are to clauses, sub-clauses, paragraphs, schedules and annexures to this Agreement;
- Use of any gender includes the other genders;
- A reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;
- Any reference to a ‘day’ (including within the phrase ‘business day’) shall mean a period of 24 hours running from midnight to midnight;
- References to a ‘business day’ shall be construed as a reference to Govt. of Odisha Working Day
- References to times are to Indian Standard Time;
- A reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and
- All headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

12.5 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

- as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;
- as between the provisions of this Agreement and the Schedules / Annexures, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules/Annexures; and
- as between any value written in numerals and that in words, the value in words shall prevail.

12.6 Law Governing Contract

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Laws of India.

12.6.1 Legal Jurisdiction

Any dispute arising out of this agreement shall be subject to the exclusive jurisdiction of courts in Bhubaneswar, Odisha.

12.6. 2 Language

This Contract has been executed in English, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

12.6.3 Notices

- Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the address specified in the SC.
- A Party may change its address for notice hereunder by giving the other Party notice in writing of such change to the address specified in the SC.
- <u>Authorized Representatives:</u> Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract by the Purchaser or the Solution Provider may be taken or executed by the officials specified in the SC.
- <u>Taxes and Duties:</u> All taxes would be paid on actuals as per applicable laws.

12.7 Fraud and Corruption

It is the Purchaser's policy to require that the Purchaser as well as Solution Provider observe the highest standard of ethics during the selection and execution of the Contract. The Purchaser also requires that the Solution Provider does not demand any service charges from the Resident unless the same is agreed with the Purchaser in advance. In pursuance of this policy, the Purchaser: Defines, for the purpose of this provision, the terms set forth below as follows:

a) "corrupt practice" means the offering, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of a public official in the selection process or in contract execution;

b) "fraudulent practice" means a misrepresentation or omission of facts in order to influence a procurement process or the execution of a contract with the Purchaser; and includes collusive practice among bidders, prior to or after proposal submission, designed to establish bid prices at artificially high or non-competitive levels and to deprive the Purchaser of the benefits of free and open competition.

c) "collusive practices" means a scheme or arrangement between two or more bidders, with or without the knowledge of the Purchaser, designed to establish prices at artificial, non-competitive levels;

d) "coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process, or affect the execution of a contract;

e) "unfair trade practices" means supply of services different from what is ordered on, or change in the Scope of Work which was agreed to;

- **Measures to be taken by the Purchaser**

a) The Purchaser may terminate the contract if it is proven that at any time the representatives or employees of the Solution Provider were engaged in corrupt, fraudulent, collusive or coercive practices during the execution of the contract, without the Solution Provider having taken timely and appropriate action satisfactory to the Purchaser to remedy the situation;

b) The Purchaser may also sanction against the Solution Provider, including declaring the Solution Provider ineligible stated period of time (as decided by purchaser), to be awarded a contract if it at any time it is proven that that the Solution Provider has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for, or in executing, a Purchaser-financed contract.

12.8 COMMENCEMENT, COMPLETION, MODIFICATION & TERMINATION OF CONTRACT

- **Term of Contract**

The term under this Contract will be for a period of 66 months which shall start from effective date of each work order.

- **Extension of Contract**
- If required by the Purchaser, an extension of the term can be granted to the Solution Provider. The final decision will be taken by the Purchaser.
- The Purchaser shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Solution Provider, at least one month before the expiration of the term hereof, whether it will grant the Solution Provider an extension of the term. The decision to grant or refuse the extension shall be at the Purchaser's discretion.
- Where the Purchaser is of the view that no further extension of the term be granted to the Solution Provider, the Purchaser shall notify the Solution Provider of its decision at least one month prior to the expiry of the Term. Upon receipt of such notice, the Solution Provider shall continue to perform all its obligations hereunder, until such reasonable time beyond the term of the Contract with the Purchaser.

- **Termination of Contract**
    - Normal termination of the contract would happen at the end of the tenure.
    - Pre-mature termination of the contract would happen in case of insolvency of bidder or due to conditions of breach happening due to reasons solely and entirely attributable to Bidder, provided prior thirty days written notice to rectify the same is given by the OCAC and failure by Bidder to rectify in the notice period.
    - Termination by Solution Provider - The Solution Provider may terminate this Contract, by not less than Ninety (90) days' written notice to the OCAC, such notice to be given after the occurrence of any of the following events.
    - If the Purchaser fails to pay any money due to the Solution Provider pursuant to this Contract and not subject to dispute pursuant to Clause hereof within forty-five (45) days after receiving written notice from the SI that such payment is overdue.
    - If the Purchaser fails to comply with any final decision reached as a result of arbitration pursuant to Clause 7.10 hereof.
    - If the Purchaser is in material breach of its obligations pursuant to this Contract and has not remedied the same within forty-five (45) days (or such longer period as the Solution Provider may have subsequently approved in writing)

following the receipt by the Purchaser of the Solution Provider's notice specifying such breach.

- OCAC failure to give acceptance of deliverables in mutually agreed time schedules

- **Effects of Termination**

- In the event of a pre-mature termination of this agreement by OCAC, the compensation payable to bidder will be decided in accordance with the Terms of Payment schedule for the milestones completed services and accepted deliverables till the last effective date of termination.
- Parties shall mutually agree upon a transition plan and comply with such a plan. The bidder shall agree to extend full cooperation in supporting the transition process.

12.8.5 Binding Clause

All decisions taken by the Purchaser regarding the processing of the Contract shall be final and binding on all parties concerned.

- **Modifications or Variations**

Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may be made by written communication between the Parties and after Prior Mutual consent by both the parties. However, each Party shall give due consideration to any proposals for modification or variation made by the other Party.

- **Force Majeure**

- Any delay in or failure of the performance shall not constitute default hereunder or give rise to any claims for damage, if any, to the extent such delays or failure of performance is caused by occurrences such as acts of godor an enemy, expropriation or confiscation of facilities by Government authorities, acts of war, rebellion, sabotage or fires, floods, explosions, terrorist activities, military operations, riots, epidemics, civil commotions, strikes etc. The Solution Provider shall keep records of the circumstances referred to above and bring these to the notice of Government of Odisha in writing immediately on such occurrences. The amount of time, if any, lost onany of these counts shall not be counted for the Contract period. The decisionof the Purchaser arrived at after consultation with the Solution Provider, shall be final and binding. Such a determined period of time will be extended by the Purchaser to enable the Solution Provider to complete the job within such extended period of time. If a Solution Provider is prevented or delayed from performing any of its obligations under the Contract with Purchaser by Force Majeure, then the Solution Provider shall notify the Purchaser the circumstances constituting the Force Majeure and the obligations of which is thereby delayed or prevented, within five (5) working days from the occurrence of the events.

- In the event the Force Majeure substantially prevents, hinders or delays a Solution Provider’s performance of Services for a period in excess of five (5) working days from the occurrence of any such event, the Solution Provider may declare that an emergency exists. Post the emergency is declared to be over, the Purchaser will communicate to the Solution Provider to resume normal services within a period of seven (7) days. In the event that the Solution Provider is not able to resume services within the next seven days, the Purchaser may terminate the Contract and/or obtain substitute performance from an alternate Solution Provider.
- Solution Provider will advise, in the event of his having to resort to this Clause,in writing, duly certified by the statutory authorities, the beginning and end of the causes of the delay, within fifteen (15) days of the occurrence and cessation of such Force Majeure.

12.9 No Breach of Contract

The failure of a Party to full fill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

Measures to be Taken

- A Party affected by an event of Force Majeure shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall takeall reasonable measures to minimize the consequences of any event of Force Majeure.
- A Party affected by an event of Force Majeure shall notify the other Party of such event as soon as possible, and in any case not later than fourteen (14) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give written notice of the restoration of normal conditions as soon as possible.
- Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

- During the period of their inability to perform the Services as a result of an event of Force Majeure, the Solution Provider, upon instructions by the Purchaser, shall either:
  - Demobilize or
  - Continue with the Services to the extent possible, in which case the Solution Provider shall continue to be paid proportionately and on pro rata basis, under the terms of this Contract.
- In the case of disagreement between the Parties as to the existence or extent of Force Majeure, the matter shall be settled according to Clause GC 8(Settlement of dispute).

12.10 OBLIGATIONS OF THE SOLUTION PROVIDER

12.10.1 Scope of Work and Deliverables

This will be in conformity with the Scope of Work and Deliverables specified in the RFP document and shall include the submissions made by the bidder in their proposal and work plans, further refined during the negotiations. Deliverables and milestones shall be established with a process of formal acceptance or measurable criteria. In case of any conflict between RFP and Proposal submitted by the Bidder in relation to Scope of Work or Deliverables, the Proposal submitted by Bidder (including clarifications, if any) shall prevail and apply.

12.10.2 Norms Governing Service Delivery

1. Provide necessary performance guarantees on signing of the agreement;
2. Shall deliver the services in a professional manner commensurate with accepted industry practices and/or technical standards which are generally expected of such an engagement;
3. Bidders shall establish a formal team structure with a named Project Manager who will serve as single point of contact and staff with competent resources to provide effective and expert service delivery, in tune to the requirements;
4. Provide a roadmap and project plan for this engagement, describing clearly the responsibilities, timelines, dependencies, milestones and risks;
5. The cost of travel & accommodation during visit to various places of Odisha for various works like system study, training etc. should be borne by the bidder.

12.10.3 Standard of Performance

The Solution Provider shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Solution Provider shall always act, in respect of any matter relating to this

Contract or to the Services, as faithful advisers to the Purchaser, and shall at all times support and safeguard the Purchaser's legitimate interests in any dealings with third Parties.

12.10.4 Conflicts of Interest

The Solution Provider/System Integrator will be barred from participating in any Bid Process (downstream activities) falling within the Scope of Work / assisted by the Solution Provider or its personnel, till the duration of their Contract with the Purchaser in the department in which the Solution Provider is providing its services under this Contract. The Solution Provider would not be barred from executing existing projects for which it is already selected within the department, however it would be barred from any future projects/ Bid Process (downstream activities) falling within the Scope of Work / assisted by the Solution Provider or its personnel, till the duration of their Contract with the Purchaser. The Solution Provider/System Integrator, if selected for any consultancy work, shall not be allowed to work in any downstream activity like application development, maintenance, support, hardware/software/tools supply etc. in the same project. Similarly, the Solution Provider/System Integrator selected as the consultant shall not be allowed to work as Solution Provider and vice-versa in the same project.

12.10.5 General Confidentiality

Except with the prior written consent of the Purchaser or its client department/organization, the Solution Provider/System Integrator and the Personnel shall not at any time communicate to any person or entity any confidential information acquired in the course of the Services, nor shall the Solution Provider and the Personnel make public the recommendations formulated in the course of, or as a result of, the Services.

12.10.6 Intellectual Property Rights (IPR)

The source code of entire applications (except OEM products/solutions) along with necessary documentations developed under this RFP/Contract should be shared with OCAC after Go-live of the application.

12.10.7 Assignment

The Solution Provider/System Integrator shall not assign, in whole or in part, their obligations under thisContract without the permission of Purchaser.

12.10.8 Force Majeure

Neither Party to this agreement shall be liable to the other for delay or default in the performance of its obligations or any loss or damage which may be suffered by the other directly due to a Force Majeure event provided that the affected Party notifies the other Party of such event and its likely effects and duration as soon as possible and takes all reasonable steps to mitigate the losses/disruption.

12.10.9 Governing Law and Jurisdiction

This agreement and all questions of its interpretation shall be construe in accordance with the Laws of India in the High Court at Cuttack having jurisdiction. Suites, if any arising out of the contract/agreement shall be filed by either party in a court of Law to which the Jurisdiction of the High Court of Odisha extends.

12.11 Audit

1. The software and documents prepared for this project are subject to audit. The bidder should help OCAC during preparation of compliances of audit without any additional cost.
2. Software including source code, licenses (if any) and all technical documents/manuals shall be in favour of the OCAC and shall be submitted tothe OCAC before final payment or on demand.
3. All records pertaining to this work shall be made available to the OCAC and its authorized agencies upon request for verification and/or audit, on the basis of a written request.

12.11.1 Good Faith

The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

12.11.2 Operation of the Contract

The Parties recognize that it is impractical in this Contract to provide for everycontingency which may arise during the life of the Contract, and the Parties hereby agree that it is their intention that this Contract shall operate fairly as between them, and without detriment to the interest of either of them, and that, if during the term of this Contract either Party believes that this Contract is operating unfairly, the Parties will use their best efforts to agree on such action as may be necessary to remove the cause or causes of such unfairness, but no failure to agree on any action pursuant to this Clause shall give rise to a dispute subject to arbitration in accordancewith Clause GC 8 hereof.

12.12 SETTLEMENT OF DISPUTES

1. The Purchaser and the Solution Provider shall make every effort to resolve amicably by direct informal negotiation on any disagreement or dispute arising between them under or in connection with the Contract.
2. If, after thirty (30) days from the commencement of such informal negotiations, the Purchaser and the Solution Provider have been unable to resolve amicably a Contract dispute, the dispute should be referred to the Chief Executive Officer, OCAC for resolution.
3. If, after thirty (30) days from the commencement of such reference, Chief Executive

Officer, OCAC have been unable to resolve amicably a Contract dispute between the Purchaser and the Solution Provider/System Integrator, either party may require that the dispute be referred to the Commissioner-cum-Secretary to Govt., E&IT Department, Govt. of Odisha.

4. Any dispute or difference whatsoever arising between the parties (Purchaser and Solution Provider/System Integrator) to the Contract out of or relating to the construction, meaning, scope, operation or effect of the Contract or the validity of the breachthereof, which cannot be resolved through the process specified above, shall be referred to a sole Arbitrator to be appointed by mutual consent of both the parties herein. In the event the parties cannot agree to sole arbitrator, such arbitrator shall be appointed in accordance with the Indian Arbitration and Conciliation Act, 1996.
5. The arbitration proceedings shall be held at Odisha and the language of the arbitration shall be English

12.13 ADHERENCE TO SAFETY PROCEDURES, RULES & REGULATIONS

1. The Solution Provider/System Integrator shall take all measures to ensure compliance with all applicable laws and shall ensure that the Personnel are aware of consequences of non-compliance or violation of laws including Information Technology Act, 2000 (and amendments thereof).
2. Statutory Audit

   a) The deliverables prepared for this project are subject to audit (by CAG or other entities). The bidder should help OCAC during preparation of compliances of audit without any additional cost.

   b) All technical documents/deliverables shall be in favour of the OCAC and shall be submitted to the OCAC before final payment or on demand.

   c) All records pertaining to this work shall be made available to the OCAC and its authorized agencies upon request for verification and/or audit, on the basis of a written request.

12.14 LIMITATION OF LIABILITY

Except in cases of gross negligence or willful misconduct: -

1. neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs,provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and
2. Maximum liability of the bidder for this project will be limited to the total valueof the contract or the amount actually paid to the bidder whichever is lower and will not include any indirect or consequential clause or damage, loss or profit, data or revenue.

12.15 INDEMNITY

1. The Solution Provider/System Integrator shall indemnify the Purchaser from and against any costs,loss, damages, expense, claims including those from third parties or liabilities ofany kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:

   a) Any negligence or wrongful act or omission by the Solution Provider or any third party associated with Solution Provider in connection with or incidental to this Contract or;

   b) Any breach of any of the terms of this Contract by the Solution Provider, the Solution Provider's Team or any third party

   c) Any infringement of patent, trademark/copyright arising from the use of the supplied goods and related services or any party thereof

2 The Solution Provider/System Integrator shall also indemnify the Purchaser against any privilege, claim or assertion made by a third party with respect to right or interest in, service provided as mentioned in any Intellectual Property Rights and licenses

3 All indemnification obligations shall be subject to the Limitation of Liability clause.

12.16 ACTION AND COMPENSATION IN CASE OF DEFAULT

Conditions for default:

a) The deliverables at any stage of the project as developed/ implemented by the Solution Provider do not take care of all or part thereof of the Scope of Work as agreed and defined under the Contract with the Purchaser.

b) The deliverables at any stage of the project as developed/ implemented by the Solution Provider/System Integrator fails to achieve the desired result or do not meet the intended quality and objective as required by the Purchaser.

c) The documentation is not complete and exhaustive.

d) There is a change in resource before the completion of a pre-defined period.

e) The Purchaser may impose penalties on the Solution Provider providing the Services as per the Service Levels defined under this Contract.

f) Any failure or delay on part of any Party to exercise right or power under this Contract shall not operate as waiver thereof.

g) The Solution Provider/System Integrator shall notify the Purchaser of any material change in their status, in particular, where such change would impact performance of obligations under this Contract.

h) The Solution Provider/System Integrator shall at all times indemnify and keep indemnified the Purchaser against all claims/damages for any infringement of any copyrights while providing its services under the Project.

i) The Solution Provider/System Integrator shall at all times indemnify and keep indemnified the Purchaser against any claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its employees or agents or by any other third Party resulting from or by any wilful action or gross negligence by or on behalf of the Solution Provider.

j) The Solution Provider/System Integrator shall at all times indemnify and keep indemnified the Purchaser against any and all claims by Employees, agent(s), employed engaged or otherwise working for the Solution Provider, in respect of wages, salaries, remuneration, compensation or the like.

k) All claims regarding indemnity shall survive the termination or expiry of the Contract.

l) All materials provided to the Purchaser by Solution Provider are subject public disclosure laws such as RTI etc. except in respect of exclusions set out in such laws.

m) The Solution Provider/System Integrator shall not make or permit to be made a public announcement or media release about any aspect of the Contract without a written consent from the Purchaser

n) The Solution Provider/System Integrator shall not assign/outsource/sub-contract the project to any other agency, in whole or in part, to perform its obligation under this agreement.

13 Formats for Response

13.1 Pre-Qualification Bid Formats

13.1.1 FORM PQ-1: Cover Letter

(To be submitted on the Letterhead of Bidder)

To
The General Manager (Admin),
Odisha Computer Application Centre,
N-1/7-D, Acharya Vihar, P.O. RRL, Bhubaneswar - 751013.

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

*Ref: RFP Reference No. - OCAC-SEGP-INFRA-0007-2022-******

Madam,

I, the undersigned, offer to provide the services for the proposed assignment in respect to your Request for Proposal No. - OCAC-SEGP-INFRA-0007-2022-******. We hereby submitour proposal which includes the pre-qualification proposal, technical proposal and commercial proposal, sealed under separate envelopes. Our proposal will be valid for acceptance up to 180 Days and I confirm that this proposal will remain binding upon us and may be accepted by you at any time before this expiry date.

All the information and statements made in our proposal are true and correct and I accept that any misinterpretation contained in it may lead to disqualification of our proposal. If negotiations are held during the period of validity of the proposal, I undertake to negotiate on the basis of proposal submitted by us. Our proposal is binding upon us and subject to the modifications resulting from contract negotiations.

I have examined all the information as provided in your Request for Proposal (RFP) and offer to undertake the service described in accordance with the conditions and requirements of the selection process. I agree to bear all costs incurred by us in connection with the preparation and submission of this proposal and to bear any further pre-contract costs. In case, any provisions of this RFP/ ToR/Scope including of our technical and financial proposal are found to be deviated, then you shall have rights to reject our proposal. I confirm that, I have the authority to submit the proposal and to clarify any details on its behalf.

I understand you are not bound to accept any proposal you receive.

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

13.1.2 FORM PQ-2: Bidder’s Organization (General Details)

(To be submitted on the Letterhead of Bidder)

Sl#	Information	Details
1.	Name of Bidder	
2.	Registered Address of Bidder	
3.	Address for Communication	
4.	Address of local office in Odisha.	
5.	Name, Designation and Address of the contact person to whom all references shall be made regarding this RFP	
6.	Mobile no. of contact person:	
7.	E-mail address of contact person:	
8.	GST Number of the Firm	
9.	PAN No. of the firm	

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

13.1.3 FORM PQ-3 [Acceptance of Terms and Conditions]

(To be submitted on the Letterhead of Bidder)

To

The General Manager (Admin),
Odisha Computer Application Centre,
N-1/7-D, Acharya Vihar P.O. RRL, Bhubaneswar - 751013.

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

Madam/Sir,

I have carefully and thoroughly gone through the Terms & Conditions along with scope of work contained in the RFP No. - OCAC-SEGP-INFRA-0007-2022-****** regardingRFP for "Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha".

I declare that all the provisions/clauses including scope of work of this RFP are acceptable to our company. I further certify that I am an authorized signatory of the company and I am, therefore, competent to make this declaration.

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

13.1.4 FORM PQ-4 [Self-Declaration against Not-Blacklisted]

(To be submitted on the Letterhead of Bidder)

To

The General Manager (Admin),
Odisha Computer Application Centre,
N-1/7-D, Acharya Vihar P.O. RRL, Bhubaneswar - 751013.

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

Ref : RFP Ref No. - OCAC-SEGP-INFRA-0007-2022-****

Sir

In response to the RFP No.: - **OCAC-SEGP-INFRA-0007-2022-****** for RFP titled "RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha", as an owner/ partner/ Director of (organisation name) ____________________________I/ We hereby declare that presently our Company/ firm is not under declaration of ineligible for corrupt & fraudulent practices, blacklisted either indefinitely or for a particular period of time, or had work withdrawn, by any State/ Central government/ PSU.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Thanking you,

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

13.1.5 FORM PQ-5: Project Citation Format

a)	Project Name:	
b)	Value of Contract/ Work Order (In INR):	
c)	Name of the Client:	
d)	Project Location:	
e)	Contact person of the client with address, phone and e-mail:	
f)	Project Duration:	
g)	Start Date (month/year): Completion Date (month/year):	
h)	Status of assignment: Completed / Ongoing (if it is on-going, level of completion)	
i)	Narrative description of the project with scope:	
j)	List of Services provided by your firm/company:	

13.1.6 FORM PQ-6: Bidder's Authorization Certificate

To (Company letter head)

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of E&IT Dept, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

Sir,

With reference to the RFP No.: - OCAC-SEGP-INFRA-0007-2022-******, Ms./Mr. <Name>, <Designation> is hereby authorized to attend meetings & submit pre-qualification, technical & commercial information as may be required by you in the course of processing the above said Bid. S/he is also authorized to attend meetings & submit technical & commercial information as may be required by you in the course of processing above said application. Her/his contact mobile number is ________________and Email id is___________________. For the purpose of validation, his/ her verified signatures are as under.

Thanking you,

Signature Verified Signature by
(Authorised Signatory) Director/CEO

Seal:
Date:
Place:
Name of the Bidder:

13.1.7 Format for Bank Guarantee for Earnest Money Deposit

To

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of E&IT Dept, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

RFP No.: - OCAC-SEGP-INFRA-0007-2022-*******

Whereas <<Name of the bidder>> (hereinafter called 'the Bidder') has submitted the bid for Submission of RFP Ref. No. - OCAC-SEGP-INFRA-0007-2022-******, for engagement of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha (hereinafter called "the Bid") to OCAC.

Know all Men by these presents that we <<Name of the Bidder>> having our office at <<Address>> (hereinafter called "the Bank") are bound unto the Odisha Computer Application Centre (hereinafter called "the Purchaser") in the sum of Rs. 1,00,00,000/- (Rupees One Crore only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.

Sealed with the Common Seal of the said Bank this <<Date>>

The conditions of this obligation are:

1. If the Bidder withdraws or amends, impairs or derogates from the tender in any respect within the period of validity of this tender; or
2. If the Bidder have been notified of the acceptance of his tender by the Purchaser during the period of its validity :-
    a. If the tenderer fails to furnish the Performance Security for the due performance of the contract; or
    b. Fails or refuses to accept/execute the contract;

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to <<insert date>> and including <<extra time over and above mandated in the RFP>> from the last date of submission and any demand in respect thereof should reach the Bank not later than the above date.

NOTHWITHSTANDING ANYTHING CONTAINED HEREIN:

i) Our liability under this Bank Guarantee shall not exceed Rs. <<Amount in figures>> (Rupees <<Amount in words>> only)

ii) This Bank Guarantee shall be valid upto <<insert date>>)

iii) It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before <<insert date>>) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:
Date:

13.2 Technical Bid Formats

13.2.1 FORM TECH-1: Description of Proposed Solution along with Technology, Scalability, Completeness and compliance details as per the specification

Bidder has to provide details of the entire solution proposed covering all requirements as listed out in this RFP.

Bidder has to specifically include (but not limited to) diagram and detailed description of the following:

a) Functional Architecture

b) Technical Architecture

c) Network Architecture

d) Deployment Architecture

e) Security Architecture

Bidder must cover all aspects of the solution while showcasing its scalability, completeness, simplicity and interoperability.

- Bidder must submit the required documents against compliance to the scope of work.
- Bidder is free to propose any type of approach for implementation of the assignment

13.2.2 FORM TECH-3: Detailed Work Plan with Activities, Duration, Sequencing, Interrelations, Milestones and Dependencies

SL#	Deliverable/ Activity*	Months							
		1	2	3	4	5	6	7	n
a)									
b)									
c)									
d)									
e)									
f)									
g)									
h)									
i)									
j)									
k)									
l)									
m)									
n)									
o)									
p)									
q)									
r)									
s)									

13.2.3 FORM TECH-4: Support Structure

Bidder to specify the support structure.

13.3 Financial Bid

13.3.1 FORM FIN-1: Financial Bid Covering Letter

(To be submitted on the Letterhead of Bidder)

To

The General Manager (Admin),
Odisha Computer Application Centre,
N-1/7-D, Acharya Vihar P.O. RRL, Bhubaneswar - 751013.

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

*Ref: RFP Reference No. - OCAC-SEGP-INFRA-0007-2022-*******

Madam/Sir,

I /We, the undersigned, offer to provide the service for provision of Cyber Security Centre of Excellence(COE) for Commissionerate of Police Bhubaneswar-Cuttack, Govt. of Odish as per RFP No.: - OCAC-SEGP-INFRA-0007-2022-****** and our Pre-Qualification, Technical and Financial Proposals. Our attached Financial Proposal is for the sum of <<Amount in words and figures>> inclusive of all applicable taxes and duties.

a) BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified in this RFP. These prices are indicated in the Financial Bid as part of this RFP response. In case there is substantial difference between the component wise price approved by OCAC and the price quoted by the bidder, OCAC will have the rights to ask the bidder to realign their prices without impacting the total bid price. We hereby agree to submit our offer accordingly.

b) PRICE AND VALIDITY

All the prices mentioned in our Tender are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this Bid are valid for a period of 5 years from the date of opening of the Bid.

We hereby confirm that our prices do not include any taxes and duties.

We understand that the actual payment would be made as per the existing tax rates during the time of payment.

c) UNIT RATES

We have indicated in the relevant forms enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

d) TENDER PRICING

We further confirm that the prices stated in our bid are in accordance with your clauses in RFP/Tender document.

e) QUALIFYING DATA

We confirm having submitted the information as required by you in your RFP. In case you require any other further information/ documentary proof in this regard before/during evaluation of our Tender, we agree to furnish the same in time to your satisfaction.

f) PERFORMANCE BANK GUARANTEE

We hereby declare that in case the contract is awarded to us, we shall submit the Performance Bank Guarantee as specified in this RFP document.

We understand you are not bound to accept any Proposal you receive. We hereby declare that our Proposal is made in good faith, without collusion or fraud and the information contained in the proposal is true and correct to the best of our knowledge and belief.

We understand that our proposal is binding on us and that you are not bound to accept any proposal you receive.

Yours faithfully,

(Authorized Signatory)
Name, Designation & Contact No.
Seal

13.3.2 Commercial bid

Sl#	Item Description/Service description	Quantity (Indicative)	Unit	Unit Cost (including GST)	Total cost (including GST)
A	B	C	D	E	F (C * E)
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
Grand Total (Excluding GST)					

Sl#	**Category**	**Quantity (Indicative)**	**Unit**	**Unit Cost (including GST)**	**Total cost (including GST)**
A	**B**	**C**	**D**	**E**	**F** **(C * E)**
Grand Total in words					

- Selection Method is Quality cum Cost-Based Selection (QCBS) with technical and commercial ratio of 70:30
- The bid price will be exclusive of all taxes and levies and shall be in Indian Rupees.
- Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail”.

13.3.3 Performance Security

To

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of E&IT Dept, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

RFP No.: **-OCAC-SEGP-INFRA-0007-2022-******

Whereas, <<name of the supplier and address>> (hereinafter called "the bidder") has undertaken, in pursuance of contract no. <Insert Contract No.> dated. <Date> to establish Cyber Security Centre of Excellence (COE) for Commossionerate of Police , Bhubaneswar, Govt. of Odisha (hereinafter called "the beneficiary")

And whereas it has been stipulated by in the agreement that the bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the agreement;

And whereas we, <Name of Bank> a banking company incorporated and having its head /registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of <<Cost of Service>> in (words) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the agreement and without cavil or argument, any sum or sums within the limits of <<Cost of Service>> (in Words) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the agreement to be performed there under or of any of the agreement documents which may be made between you and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification. This Guarantee shall be valid until <<<insert date>>

Notwithstanding anything contrary contained in any law for the time being in force or banking practice, this guarantee shall not be assignable or transferable by the beneficiary i.e OCAC. Notice or invocation by any person such as assignee, transferee or agent of beneficiary shall not be entertained by the Bank.

NOTHWITHSTANDING ANYTHING CONTAINED HEREIN:

i) Our liability under this bank guarantee shall not exceed <<amount>> (Amt. in words).
ii) This bank guarantee shall be valid up to <<insert date>>.
iii) It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <<insert date>> failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:
Date:

14 Proposed Master Service Agreement

Master Service Agreement for System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

This agreement is made on_____/_____/________between Odisha Computer Application Centre, the Designated Technical Directorate of Electronics and Information Technology Department, Government of Odisha having its office at Plot-N-1/7-D, Po- RRL, Acharya Vihar Square, Bhubaneswar - 751013, Odisha. (hereinafter called **“Purchaser” or “OCAC”**) which expression shall unless repugnant to the context thereof include his successors, heirs, assigns, administrator, executive & representative of the one part,

And

M/s______________________________, a company registered under the Provisions of Act,1956____________is having its registered office at ____________________ India (hereinafter called **“Solution Provider”**) which expression shall unless repugnant to the context thereof include his successors, heirs, assigns, administrator, executive and representatives of the other part.

WHEREAS OCAC had invited Request for Proposal (RFP) for engagement of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha vide RFP Reference No.________________________________. Based on the tender evaluation, M/s ___________________has been selected as **“Solution Provider”.**

And in "pursuance of above facts the parties have agreed to enter into this agreement.

NOW THIS AGREEMENT WITNESSES AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Contract referred to.
2. The following documents (collectively referred to as “Contract Documents”) shall be deemed to form and be read and construed as part of this Agreement, viz.:
   a) RFP floated by OCAC Reference No.________________________, Technical bid and Commercial furnished by Solution Provider with respect to RFP
   b) The General Conditions of Contract
   c) The Special Conditions of Contract
      i) Following Appendix to GC and SC:
      ii) Appendix-A: Scope of Work
      iii) Appendix-B: Deliverables
      iv) Appendix-C: Cost of Service

d) The mutual rights and obligations of the Purchaser and the Solution Provider shall carry out the Services in accordance with the provisions of the Contract;

IN WITNESS WHEREOF, the Parties hereto have caused this Contract to be signed in their respective names as of the day and year above written.

On behalf of Purchaser	On behalf of Solution Provider
Signature: Name: Designation:	Signature: Name: Designation:
Witness -1 Name & Address:	Witness -1 Name & Address:
Witness -2 Name & Address:	Witness -2 Name & Address: