



DIGITAL FORENSICS EXAMINATION REPORT

Prepared By:

21MEI10056 : JATIN AGRAWAL
21MEI10060 : KULDEEP KUMAR JHA
21MEI10027 : VIKAS TOMAR
21MEI10021 : PANKAJ KUMAR
21MEI10003 : ANSHUL PATIDAR
21MEI10052 : LALIT SAHU

Advisor: Prof. (Dr.) Shishir Kumar Shandilya, Deputy Director – SECURE, VIT Bhopal

Submission Date: OCT. 15, 2022

VIT BHOPAL UNIVERSITY, INDIA

Disclaimer: The chosen case scenario is for learning purposes only and any association to an actual case and litigation is purely coincidental. The evidence presented in the case scenario is fictitious and is not intended to reflect actual evidence. Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the Indian Central and State governments, and the information and statements shall not be used for the purposes of advertising.

Table of contents:

S.NO.	CONTENTS	PAGE-NO.
1.	Investigator(s)	3
2.	Case Details	4
3.	Case Background	5
4.	Suspect Summary	8
5.	Legal Issues	8
6.	Evidence #1	9
7.	Evidence #2	10
8.	Evidence #3	11
9.	Evidence #4	12
10.	Evidence Analysis	14
11.	Processing Location	15
12.	Storage of Evidence	16
13.	Evidence Collected	17
14.	Evidence Examination Steps	18
15.	Appendix A: Chain of custody	21
16.	Deleted Evidences	22
17.	Appendix B: Consultation Letter	24
18.	Appendix C: References	25


Investigator (s):	
1.	<p>Name: JATIN AGRAWAL Badge/ID: 21MEI10056 Specialization: Specialization in Digital Forensic with 7-year Experience. Date when deputed on the case: 01-Sep. -2022 Deputed by: VIT BHOPAL Relieving Date: 25-OCT-2022</p>
2.	<p>Name: KULDEEP KUMAR JHA Badge/ID: 21MEI10060 Specialization: Specialization in digital forensic with 7-year Experience. Date when deputed on the case: 01-Sep. -2022 Deputed by: VIT BHOPAL Relieving Date: 25-OCT-2022</p>
3.	<p>Name: VIKAS TOMAR Badge/ID: 21MEI10027 Specialization: Specialization in digital forensic with 6-year Experience. Date when deputed on the case: 01-Sep. -2022 Deputed by: VIT BHOPAL Relieving Date: 25-OCT-2022</p>
4.	<p>Name: PANKAJ KUMAR Badge/ID: 21MEI10021 Specialization: Specialization in digital forensic with 5-year Experience. Date when deputed on the case: 01-Sep. -2022 Deputed by: VIT BHOPAL Relieving Date: 25-OCT-2022</p>
5.	<p>Name: ANSHUL PATIDAR Badge/ID: 21MEI10003 Specialization: Specialization in digital forensic with 7-year Experience. Date when deputed on the case: 01-Sep. -2022 Deputed by: VIT BHOPAL Relieving Date: 25-OCT-2022</p>
6.	<p>Name: LALIT SAHU Badge/ID: 21MEI10052 Specialization: Specialization in digital forensic with 6-year Experience. Date when deputed on the case: 01-Sep. -2022 Deputed by: VIT BHOPAL Relieving Date: 25-OCT-2022</p>

Case Details	
Case Number:	FIR-15529
FIR Date:	15 th OCT. 2022
Lead Investigating Officer:	Dr. Shishir Kumar Shandilya
Prime Offense:	COMPROMISED SECURITY SYSTEM
IPC Sections:	121, 201, 425
IT Act Sections:	72, 43, 66, 66 b, 66c, 66d, 66f
Other Acts:	N.A.
Crime Scene Location:	PRIME MINISTER OFFICE, SOUTH BLOCK, RAISINA HILL, NEW DELHI.
# of Evidence seized:	10
# of Digital Evidence seized:	10
Date of Request of Examination:	15 th OCT. 2022
Date of Conclusion:	25 th OCT. 2022
Abstract	The purpose of this report is to provide examination procedures, findings, and recommendations from fictitious evidence regarding compromise in the security system of PM Office. This information provides for the presentation stage of an investigation. Included in the report are the digital forensic standards, principles, methods, and legal issues that may impact the court's decision. The creation of the report is unbiased, and intends to assist the court make a judgment of Mr. Rakesh kr. Singh, Mr. Vikram Rathore, Mr. Abdul Siddiqui. This written report provides detail for the evidence. The focus of this report is on the digital evidence collected from the mentioned three suspects. Therefore, the report omits the physical evidence collected from security room. References to evidence items collected by the investigator may be referred in this report.
Accused #1	Name: Mr. Rakesh kr. Singh Offense: Data leaking, Terrorist connection
Accused #2	Name: Mr. Vikram Rathore Offense: Evidence hiding, Terrorists connection
Accused #3	Name: Mr. Abdul Siddiqui Offense: system hacking, Terrorist connection
Special Note (if any)	N.A.


Case Background (Detailed)	<p>On 15th OCT. 2022, An anomalous behavior in security system was observed by the concern staff of P.M.O security office. The search operation for the security flaws had started by digital forensic team. During operation two unknown active systems (laptop) were found inside. The systems were connected to the LAN and actively making copy of all the confidential data from the network, also in another system the data was continuously manipulated and unusual requests over network was generating to divert the attention of concern authority. Storage devices like two SSD disks, Rubber Ducky for nefarious input commands seized also. During investigation procedure some security staff tried to cover up the unknow system connected to the network. Hence, three newly assigned security engineers were the prime suspects. After investigation the suspect’s laptops and the mobile phones were seized for forensic investigation. In our investigation, from seized evidence we found that all the suspects were involved in leaking confidential data of government. For this they all were being paid by several terror organization. In the network logs of seized evidences, we found that they were regular visitor the several terrorists group’s website as well. There were several transaction confirmations mails from unknown source in their respective devices.</p> <p>On the basis of analysis of evidence, (Mr. Rakesh kr. Singh, Mr. Vikram Rathore, Mr. Abdul Siddiqui) on 17thOCT. 2022 police arrested them in case of confidential data leaking, promoting terrorism, system hacking, evidence hiding, terrorist group connection.</p> <p>The seizure of the suspect’s devices was performed in a manner consistent with recommendations found in Electronic Crime Scene Investigation: A Guide for First Responders. The investigation was conducted in accordance with processes outlined by the National Institute of Justice (NIJ) and the Technical Working Group for the Examination of Digital Evidence (TWGEDE). The investigation officers use the tools like log analyzer, autopsy, magnet acquire, FTK Imager and EnCase Mobile Manage to track all the past activity as well as recovery of data from seized evidence.</p>		
Suspect summary			
Priority	Suspect	Charges	Bail Bond
1	Mr. Rakesh kr. Singh	Data leaking, Terrorist connection	—
2	Mr. Vikram Rathore	Evidence hiding, Terrorists connection	—

3	Mr. Abdul Siddiqui	system hacking, Terrorist connection	—
Legal Issues			
Topic		Topic	Topic
ADMISSABILITY OF EVIDENCE:		Most difficult part of the case will be the admissibility of content. presenting evidence in the court which will be admissible. So, evidence should be transparent which directly indicates suspect a guilty.	
AUTHENTICATING EVIDENCE:		Authenticating digital evidence may be a challenge as the court may not understand the complexity in various digital communications. It refers to providing sufficient evidence for a reasonable juror to conclude the case.	

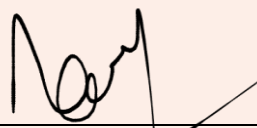
Evidence # 1		
Objective	To find copied confidential data	
Device Type	hp Laptop	
Serial Number	S234A	
Operating System	Window 10	
Offense	Data Breaching, Terrorist connection	
Investigating Officer	JATIN AGRAWAL / KULDEEP KUMAR JHA	
Chain of Custody	Refer to Appendix A	
Tools Used	Autopsy, network logs analyzer	
Assessment	<ul style="list-style-type: none"> ➤ Legal Authority Established ➤ Chain of Custody Documented ➤ Request for Service Documented ➤ Equipment for Analysis Available in Lab 	
Acquisition	<ul style="list-style-type: none"> • Copy of confidential data received. • Logs indicating connection from terrorists' servers. 	
Examination	15/OCT/2022 17:00, Starting to Examine the laptop 15/OCT/2022 17:05, Analyze the laptop by using autopsy. 15/OCT/2022 17:10, Also analyze using network analyzer 15/OCT/2022 17:21, Found some irrelevant data sharing	
Documentation and Reporting	Found the data transfer between unknown server	
Hash Values	Filename	Value
	MItry_prjct.pdf	2da0b2a7be801f96a143a88c4ef063a8
	transc_1.png,	9c75e5c43e75ddab591foa458e75070
	tranc_2.png, trans_3.png	obcfob991a4b62f911e28cf404cf9c57 70414a27d92e628157396145d1346f13

Examiner's Comments	<p>We analyzed a HP laptop properly by using Autopsy tool, and come to know that the data confidentiality is not followed, and data is shared between some irrelevant servers.</p> <p style="text-align: right;">  Examiner's Sign </p>
---------------------	---


Evidence # 2		
Objective	To find copied confidential data	
Device Type	ASUS Laptop	
Serial Number	S235B	
Operating System	Windows 10	
Offense	Data hiding, Terrorist connection	
Investigating Officer	Vikas Tomar / Pankaj Kumar	
Chain of Custody	Refer to Appendix A	
Tools Used	Autopsy, Wireshark	
Assessment	<ul style="list-style-type: none"> ➤ Legal Authority Established ➤ Chain of Custody Documented ➤ Request for Service Documented ➤ Equipment for Analysis Available in Lab 	
Acquisition	<ul style="list-style-type: none"> • Multiple unnecessary requests on the network. • Malicious Executive files 	
Examination	16/oct/2022 14:00, Examine the Laptop 16/oct/2022 15:05, Analyze using Wireshark network analyzer 16/oct/2022 15:015, Found some unnecessary request on the network.	
Documentation and Reporting	Unnecessary request on server	
Hash Values	Filename	Value
	REQUESTS.PY	5b5e7b4e4dd18ecab2337894d4b9da4a
	GENERATE_404.PY	f6399faf8c54ab78dd6419ab7a055e14

Examiner's Comments	<p>We analyzed a HP laptop properly by using Wireshark tool, and come to know that the some server have unnecessary request and found some malicious code files which leads to continuous request generation.</p> 	
	Examiner's Sign	

Evidence # 3		
Objective	To Get some important evidence	
Device Type	SSD	
Serial Number	S2VF856	
Operating System	N.A.	
Offense	Stealing data of government project.	
Investigating Officer	ANSHUL / LALIT SAHU	
Chain of Custody	Refer to Appendix A	
Tools Used	Autopsy, Smartmono tools	
Assessment	<div>➤ Legal Authority Established</div> <div>➤ Chain of Custody Documented</div> <div>➤ Request for Service Documented</div> <div>➤ Equipment for Analysis Available in Lab</div>	
Acquisition	Found some important data that can to break data integrity in PMO office.	
Examination	17/OCT/2022 12:45, Examine the SSD. 17/OCT/2022 13:05, Analyze that SSD using smartmono tools. 17/OCT/2022 13:40, Found some irrelevant data.	
Documentation and Reporting		
Hash Values	Filename	Value
	Mltry_prjct.pdf	2da0b2a7be801f96a143a88c4ef063a8
	RBI_change_in_guid.docs	1cff671e65f8ad426d18f8df2037264c
	ORDER_HOME_MNS.DOCS	3d056ff9e6dc167a34376864coe98434

Examiner's Comments	<p>After examining this SSD, we get to know that this SSD has the data related to government projects, and publication that can break the CIA of PMO office data.</p> <p style="text-align: right;"></p>
	Examiner's Sign

Evidence # 4		
Objective	Analyzing of input commands	
Device Type	Rubber Ducky USB	
Serial Number	OA1569F	
Operating System	N.A.	
Offense	It contains malicious code for root access of system that work as an input.	
Investigating Officer	JATIN AGGRAWAL/ KULDEEP KUMAR JHA	
Chain of Custody	Refer in Appendix A	
Tools Used	Autopsy	
Assessment	<ul style="list-style-type: none"> ➤ Legal Authority Established ➤ Chain of Custody Documented ➤ Request for Service Documented ➤ Equipment for Analysis Available in Lab 	
Acquisition	<ul style="list-style-type: none"> ● Some irrelevant program that can help in breaching of data. 	
Examination	<p>18/OCT/2022 18:00, Examine the Rubber Ducky.</p> <p>18/OCT/2022 18:10, Get some program that breach the data.</p>	
Documentation and Reporting	Found the irrelevant program.	
Hash Values	Filename	Value
	Input_request.py	892291cecc4c984427f6595f0dcb885c

Examiner's Comments	<p>After examining this Rubber Ducky, we get to know that this rubber ducky has the malicious program that can work as a input and can help for data breaching.</p> 
	Examiner's Sign

Behavioral Evidence Analysis	
<p><i>In this case all the evidences like: Smart phones, laptops, SSD, Rubber ducky etc. , collects by the suspects and analyzed by all the investigators by using several tools like Autopsy, Wireshark, Smartmonotools etc. and we get to know that the given findings were there:</i></p>	
Findings	
Finding #1	Found some irrelevant programs that helps to break data integrity in PMO office.
Finding #2	Multiple unnecessary requests on the network.
Finding #3	Malicious Executive files.
Finding #4	Copy of confidential data received.
Finding #5	Logs indicating connection from terrorists' servers.
Finding #6	Some data related to governmental upcoming plans like: official projects, military projects, economy distributions etc.
Recommendations	

The jury should consider Mr. Rakesh kr. Singh, Mr. Vikram Rathore, Mr. Abdul Siddiqui as the prime perpetrators of the case and we get the evidence collected on their laptops, phones, SSD, Rubber ducky. The evidence proves that these three are trying to breach the security of PMO office, and trying to leak the confidential data. Also there was major transactions history obtained from suspects devices, which indicates their The evidence obtained shows that they are trying to do something big, with terrorist group, so this will prove that these are the suspects of this case.

2da0b2a7be801f96a143a88c4ef063a8 9c75e5c43e75ddab591foa458e75070 0bcf0b991a4b62f911e28cf404cf9c57 70414a27d92e628157396145d1346f13 2da0b2a7be801f96a143a88c4ef063a8 1cff671e65f8ad426d18f8df2037264c	
Hash Value	Sign of Lead Digital Investigator with date

PROCESSING LOCATION:

Evidence was processed at the NCFL-E (DIGITAL FORENSIC DIVISION). NCFL-E(National Cyber Forensic Laboratory for Evidentiary purpose) at CFSL, Hyderabad has been created by upgrading the existing Digital Forensic Facility under the 'Center for Cybercrime Prevention against women and children' (CCPWC) scheme of MHA.

CFSL STANDS FOR CENTRAL FORENSIC SCIENCE LABORATORY



Due to the quality of the laboratory, the court can be assured that:

- ✓ Evidence will be well documented
- ✓ Appropriate packaging, transport, and storage of evidence
- ✓ Storage locations are free from electromagnetic interference and damaging substances
- ✓ Continually assess the quality and condition of the devices

STORAGE OF EVIDENCE:

Items are placed in a heavy-duty mechanical evidence locker room. Fingerprint security system into the room allows that both deposit and retrieval can only be performed by pre-authorized individuals whose prints have already been entered into the system. Lockers are divided into readily identifiable compartments, which are opened and closed with the user-friendly button locks. A heavy-duty steel structure, with welding at the ends to reinforce the strength of the doors. The doors themselves incorporate robust load-bearing hinges and rubber stops to ensure smooth closure. The digital lockers are also enhanced with detection sensors and LED panels that display valuable information at a glance.



Appendix A: Chain of Custody

Property Record Number:

102

KOTA, Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: HR-15529 Offense: Terrorist Connections, Confidential
 Submitting Officer: (Name/ID#) Kuldeep Kumar Jha (21MEI10060) data breach.
 Victim: _____
 Suspect: Mr. Rakul K. Singh, Mr. Vikram Rathan, Mr. Abdul Siddiqui
 Date/Time Seized: 15th OCT. 2022 Location of Seizure: P.M.O, South Block, Raisina hill.
(14:00 PM)

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1.	1	HP laptop (PAVILLION, S934A, Good condition, no marks)
2.	1	ASUS laptop (TUF, PF2PP169, Good condition, no marks)
3.	2	SSD (Samsung, SM960E856, Good condition, dent)
4.	1	Router Switch (HAK-5 WR062, Good condition, n.a)
5.	2	Mobile phones (Realme, AS2489, Good condition, no marks) " (Redmi, PMS32, Good condition, broken notch.)
6.	3	Laptops (HP VICTUS, S9269A, Good condition, no marks) Dell, G58299A, Good condition, no marks (Lenovo, 8XZTPR6, Good)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
1,2	15 OCT. 2022 17:30 PM	Kuldeep K. Jha (21MEI10060) <i>[Signature]</i>	Jatin Agarwal (21MEI10050) <i>[Signature]</i>	Seized, P.M.O
3,4	15 th OCT. 2022 15:30 PM	Pankaj Kumar (21MEI10061) <i>[Signature]</i>	Anshul Ratan (21MEI10053) <i>[Signature]</i>	Seized, P.M.O under used.
5,6	15 th OCT. 2022 17:30 PM	(21MEI10060) <i>[Signature]</i> Kuldeep K. Jha	(21MEI10050) <i>[Signature]</i> Jatin Agarwal	Seized, P.M.O collected from suspects.

Appendix B: Consultation Letter:

DATE: 06/30/2018

TO: Dr. Shishir Kumar Shandilya

FROM: JATIN, KULDEEP, VIKAS, LALIT, ANSHUL, PANKAJ

SUBJECT: Consultation of Digital Evidence for Case FIR_15529

The purpose of the document is to inform you (case investigator) what may or may not be discovered. Additionally, we will explore preliminary topics in digital analysis relevant to this case. From the request placed by your team, I see no other forensic processes required for the evidence. This includes all items listed: laptops, cell phone, SSD, Rubber ducky. I recommend the possibility of pursuing a preservation order to the suspected Internet service provider (ISP) to identify the IP address and application used to access the internet. The potential evidence being sought remains to be images, messages, emails, social media artifacts, and other information related to the data breaching, data hiding, terrorists' connection. Evidence may need to be retrieved through interview/interrogation, existing documents, or by using applications designed to find deleted files of the device. From our understanding, the suspects have a high level of understanding of computers. Therefore, there is reasonable doubt no concealment or destruction programs were deployed on the devices and no additional specialized personnel will be needed. The evidence priority requested by your team is noted. Evidence analysis will begin with two unknown devices, the lead suspect for threatening and kidnapping of the victim. Second, we will inspect the devices of SSD, suspected of unlawful disclosure or promotion of intimate visual material. If These suspects covers other criminal activity unrelated to charges in case FIR_15529, we will be looking for further guidance from your team.

Sincerely,

JATIN, KULDEEP, VIKAS, LALIT, ANSHUL, PANKAJ

Digital Forensic Investigator(s)

Appendix C: References:

1. forensic report , 10-July-2017, Evidence analysis in case #90033.
2. Chain of Custody Tracking form: <https://sec-form-144.pdfFiller.com/>

~END OF REPORT~