DIGITAL FORENSICS EXAMINATION REPORT

Prepared By: Devangana Sujay, Arpit Sivakumar, Raghunandan Tomar, Muskaan Bhotika, Ananya Das, Sujal Kothari

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

Submission Date: October 6, 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.

Investigator (s):

Name: Devangana Sujay
Badge/ID: 21MEI10007
Specialization: Evidence Management
Date when deputed on the case: September 13, 2022
Deputed by: VIT Bhopal University
Relieving Date: October 4, 2022

Name: Arpit Sivakumar
Badge/ID: 21MEI10018
Specialization: Asset Analyst
Date when deputed on the case: September 13, 2022
Deputed by: VIT Bhopal University
Relieving Date: October 4, 2022

Name: Raghunandan Tomar
Badge/ID: 21MEI10024
Specialization: Evidence Examiner
Date when deputed on the case: September 13, 2022
Deputed by: VIT Bhopal University
Relieving Date: October 4, 2022

Name: Muskaan Bhotika
Badge/ID: 21MEI10029
Specialization: Lead Digital Investigator
Date when deputed on the case: September 13, 2022
Deputed by: VIT Bhopal University
Relieving Date: October 4, 2022

Name: Ananya Das
Badge/ID: 21MEI10033
Specialization: Digital Forensic Examiner
Date when deputed on the case: September 13, 2022
Deputed by: VIT Bhopal University
Relieving Date: October 4, 2022

Name: Sujal Kothari
Badge/ID: 21MEI10061
Specialization: Evidence Examiner
Date when deputed on the case: September 13, 2022
Deputed by: VIT Bhopal University
Relieving Date: October 4, 2022

Case Details

Case Number:	**221.2**
FIR Date:	**May 3, 2022**
Lead Investigating Officer:	Dr. Shishir Kumar Shandilya
Prime Offense:	**Murder**
IPC Sections:	**204, 205, 302, 328, 354 D, 419, 507**
IT Act Sections:	**66 A, 66 D, 66 E**
Other Acts:	**Cyberbullying, Impersonation**
Crime Scene Location:	**Room # 342, Highway Garden Hotel, NH Bypass, Padivattom, Edappally, Cochin, Kerala, India – 682024**
# Of Evidence seized:	8
# Of Digital Evidence seized:	4
Date of Request of Examination:	**September 6, 2022**
Date of Conclusion:	**October 4, 2022**
Abstract	A body of a girl was found in a hotel room that was turning blue, indicating that the victim had died due to poisoning. This ruled out health issues as cause of death. During the investigation, it was revealed that the victim, Anju Srivastava was murdered by Mohit Sharma as she had bullied his sister, Mallika Sharma as a result of which Mallika had committed suicide. Mohit vowed to avenge her death. So, he planned to get close to Anju and then kill her.
Accused #1	**Name:** Mohit Sharma **Offence:** Murder, Cyberbullying, Impersonation
Special Note (if any)	

Case Background (Detailed)	A body of a girl was found in a hotel room that was turning blue, indicating that the victim had died due to poisoning. This ruled out health issues as cause of death. During the investigation, it was revealed that the victim, Anju Srivastava was murdered by Mohit Sharma as she had bullied his sister, Mallika Sharma as a result of which Mallika had committed suicide.

Suspect Summary

Priority	Suspect	Connection	Charges	Bail Bond
1	Mohit Sharma	Boyfriend	Murder Cyberbullying Impersonation	Non-bailable cognizable offence
2	Ashutosh Srivastava	Father	Murder	Non-bailable cognizable offence
3	Kanishka Srivastava	Mother	Murder	Non-bailable cognizable offence

Legal Issues

Topic	Authority/Rule	Description
Admissibility of Evidence	Section 65 B(1)	Information contained in electronic record, which is being stored, recorded or copied as a computer output shall be deemed as document and shall be admissible as evidence.
Authenticating Evidence	Section 65 B(4)	It may be an issue as the court may not be able to understand the complexity of the various digital evidence.

Evidence # 1 – Mobile phone of Anju Srivastava

Objective	To determine that she was cyberbullied by Mohit Sharma
Device Type	Redmi Note 10 Pro
Serial Number	NN572LL/A
Operating System	Android
Offense	Cyber Bullying , Impersonation, Murder
Investigating Officer	Devangana Sujay
Chain of Custody	Refer to Appendix A
Tools Used	DroidKit, Android Studio
Assessment	✓ Legal Authority Established ✓ Chain of Custody Documented

	✓ Request for Service Document ✓ Equipment for Analysis Available in Lab
Acquisition	The configuration of the phone was documented and the data was duplicated multiple times in a manner that preserved original data.
Examination	16/08/2022 10.00 - The phone was unlocked using DroidKit. 16/08/2022 13.30 - Initialization of Mobile Forensics. Write blocker was utilized. With the help of Android Studio , proceeded with the evaluation of the device. 16/08/2022 17.00 - Call logs were checked. 2 calls from above mentioned unknown number was identified. On WhatsApp messenger, conversations with the same number are discovered. 17/08/2022 9.00. - 17/08/2022 12.00 - Created timeline of events
Documentation and Reporting	Material items were reported in the "Findings" section of this document
Examiner's Comments	On examining Ms. Anju Srivastav's phone, it was discovered from her WhatsApp chats with the suspect that she was cyber bullied by him .The phone number of the suspect was obtained by this examination - " +447975777666 ". Other social medias were check in order to collect further evidence but were proven futile in reference to this case.
	Examiner's Sign
Evidence # 2 – Laptop of Anju Srivastav	
Objective	To determine whether Anju Srivastav was cyberbullied by Mohit Sharma
Device Type	HP Pavilion x360
Serial Number	4CE0460D0G
Operating System	Windows 11
Offense	Cyber Bullying
Investigating Officer	Raghunandan Tomar
Chain of Custody	Refer to Appendix A
Tools Used	RAM Capture, ExifTool
Assessment	✓ Legal Authority Established ✓ Chain of Custody Documented ✓ Request for Service Document ✓ Equipment for Analysis Available in Lab

Acquisition	The configuration of the laptop was documented and the data was duplicated multiple times in a manner that preserved original data.
Examination	17/08/2022 10.15 - From gallery, photo of Mallika Sharma with Anju Srivastav was identified 17/08/2022 - Social media platforms were checked and connections with Anju Srivastav are detected. 7/19/08/2022 10.15 - No other relevant data related to the case was found out. Hence proceeded with recording of timeline of events.
Documentation and Reporting	Material items were reported in the "Findings" section of this document
Examiner's Comments	After examination, a picture of Anju Srivastav and Mallika Sharma and social media connections were discovered. No other evidences were obtained from this device that are relevant.
	RThomas Examiner's Sign
Evidence # 3 – Mobile phone of Mohit Sharma	
Objective	To find out evidence to prove that the suspect is the killer
Device Type	One Plus Nord 2T 5G
Serial Number	f1e65cf2
Operating System	Oxygen OS
Offense	Impersonation, Murder
Investigating Officer	Sujal Kothari
Chain of Custody	Refer to Appendix A
Tools Used	ExifTool , Autopsy 4.19.3
Assessment	✓ Legal Authority Established ✓ Chain of Custody Documented ✓ Request for Service Document ✓ Equipment for Analysis Available in Lab
Acquisition	The configuration of the phone was documented and the data was duplicated multiple times in a manner that preserved original data.
Examination	21/08/2022 11.15 WhatsApp conversations obtained from Anju Srivastav's phone are discovered to have been send from this device as well. 21/08/2022 16.00 Identical call logs are coincided with those received by Anju Srivastav 22/08/2022 12.15 No other records related to the case were discovered. 22/08/2022 15.15 Created the timeline of events of the case.

Documentation and Reporting	Material items were reported in the "Findings" section of this document
Examiner's Comments	Upon the examination conducted, the calls and messages coincide proving that Mohit Sharma was cyberbullying Anju Srivastav. No other suspicious data was recovered from the investigation.
	Examiner's Sign
Evidence # 4 – Laptop of Mohit Sharma	
Objective	To prove that the suspect is the killer
Device Type	Dell Inspiron 3511
Serial Number	4F34DG1
Operating System	Windows 10
Offense	Cyberbullying, Murder
Investigating Officer	Devangana Sujay
Chain of Custody	Referred to chain of custody – Appendix
Tools Used	Autopsy 4.19.3
Assessment	✓ Legal Authority Established ✓ Chain of Custody Documented ✓ Request for Service Document ✓ Equipment for Analysis Available in Lab
Acquisition	The configuration of the laptop was documented and the data was duplicated multiple times in a manner that preserved original data.
Examination	17/08/2022 14.15 Using RAM Capture volatile memory of the device was retrieved. 18/08/2022 16.30 Recycle bin was checked and a copy of a downloaded pdf document was obtained. 18/08/2022 19.00 ExifTool was used on the pdf document to obtain metadata 19/08/2022 Created timeline of events.
Documentation and Reporting	Material items were reported in the "Findings" section of this document

Examiner’s Comments	On examination of Mr. Mohit Sharma's laptop , suicide note of his sister was obtained from the recycle bin. This proves to be a lead in the case making it clear that it was Mohit Sharma who murdered Anju Srivastav in order to take revenge on his sister's death.
	Examiner’s Sign

Behavioral Evidence Analysis

Behavioral Evidence Analysis was completed alongside the digital forensic examination. BEA is done to ascertain the suspect(s) motivation and help identify the patterns in evidence associated with their profile. The four steps to conduct BEA are:

1. Forensic Analysis (see section “Evidences”)
2. Victimology
3. Crime scene characteristics
4. Offender Characteristics

2. **Victimology:** Defined as investigating, establishing, and evaluating victim traits and history, the process of victimology can help identify the culprit as soon as possible. The characteristics of victim can shed light on the offender’s motive, modus operandi, knowledge, and skills.

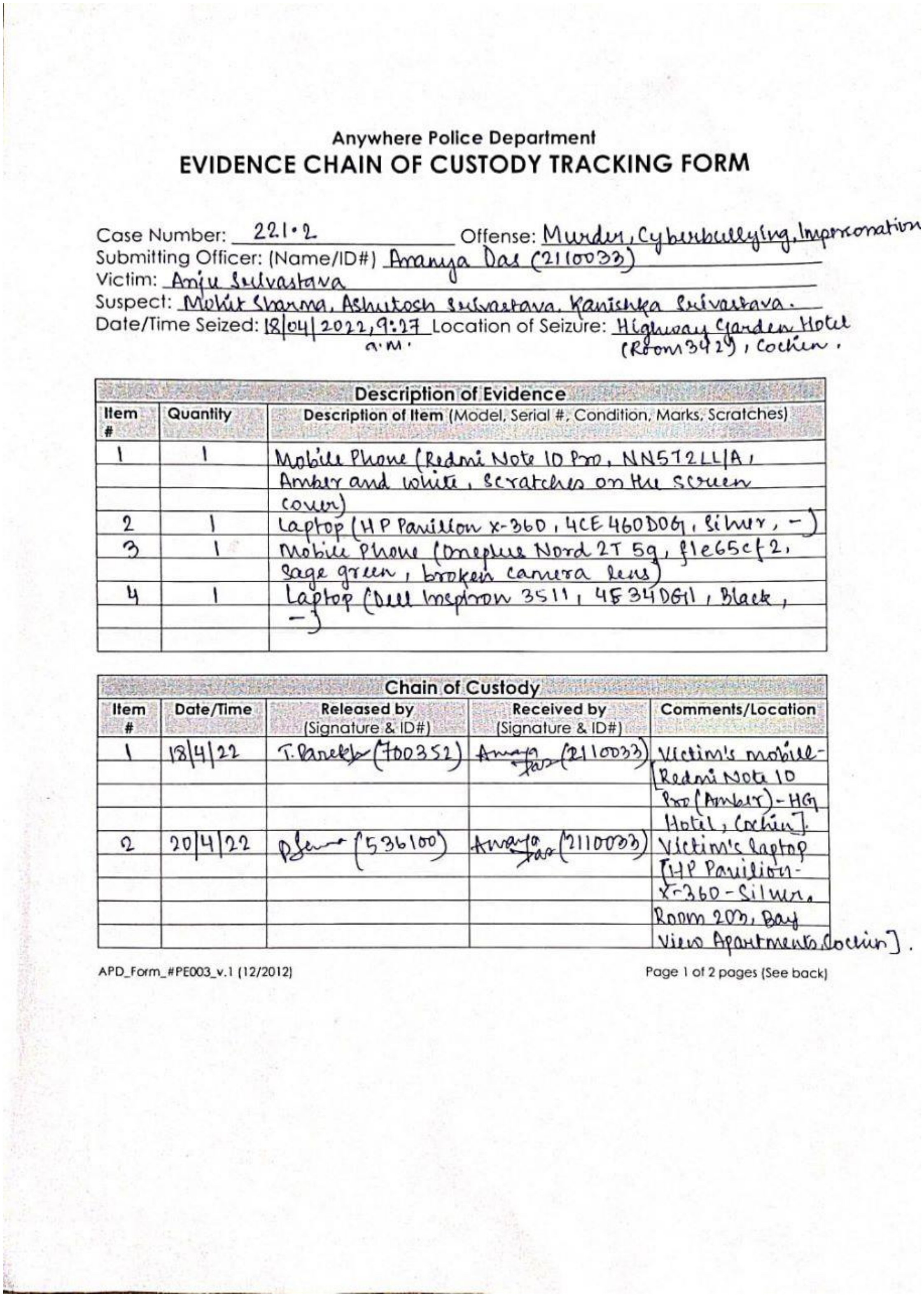
> 2.1 Exposure Assessment: the accessibility of the internet has increased the chances of harming others with digital stalking and impersonation. Upon befriending Anju, and subsequently becoming her boyfriend, Mohit has access to her accounts, thus enabling him to easily cyberstalk her befriend her by impersonating.

3. **Crime Scene Characteristics:** Sharma primarily used Instagram, Snapchat and Tinder to stalk Anju. The account document holding the login/passwords to fake brandy files indicate other victims subject to impersonation and stalking.

4. **Offender Characteristics:** The analysis of the social media accounts showed that Sharma used flattery to gain attention from Anju. Once he succeeded in gaining her attention, he proceeded to manipulate her into meeting him in Highway Garden Hotel. Sharma often complimented Anju on anything she posted on her social media handles, indicating that he stalked the girl on the internet.

<table>
<tr><th colspan="2">Findings</th></tr>
<tr><td>Finding #1</td><td>From the mobile of Anju, it was discovered that she was cyberbullied by Mohit who had impersonated to be an unknown stalker of hers. Chats and call logs clarify the same.</td></tr>
<tr><td>Finding #2</td><td>Anju's laptop contained a picture of Anju and Mallika proving the link between the two.</td></tr>
<tr><td>Finding #3</td><td>Examining Mohit's mobile phone, the calls and chat records justify the findings #1 because it coincides the evidences found from Anju's phone. This is the final proof that is submitted to prove that he is the murderer.</td></tr>
<tr><td>Finding #4</td><td>From Mohit's laptop, suicide note of his sister, Mallika was found. The note stated that the reason for suicide was Anju and her friends. Hence, it is clear that Mohit had planned a revenge to avenge the death of his sister.</td></tr>
<tr><th colspan="2">Recommendations</th></tr>
<tr><td colspan="2">The jury should consider Mohit Sharma as the prime accused in the case of murder of Anju Srivastava due to the fact that all evidences retrieved prove him to be the culprit. The evidences collected show him to be a cyber stalker with an intent to lure Anju under false pretenses and carry out the heinous act of murder.
The evidence obtained show no intent to distribute explicit images. There's no evidence that her parents were</td></tr>
<tr><td></td><td>Muskaan
4.10.2022</td></tr>
<tr><td>Hash Value</td><td>Sign of Lead Digital Investigator with date</td></tr>
</table>

Appendix A: Chain of Custody



Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

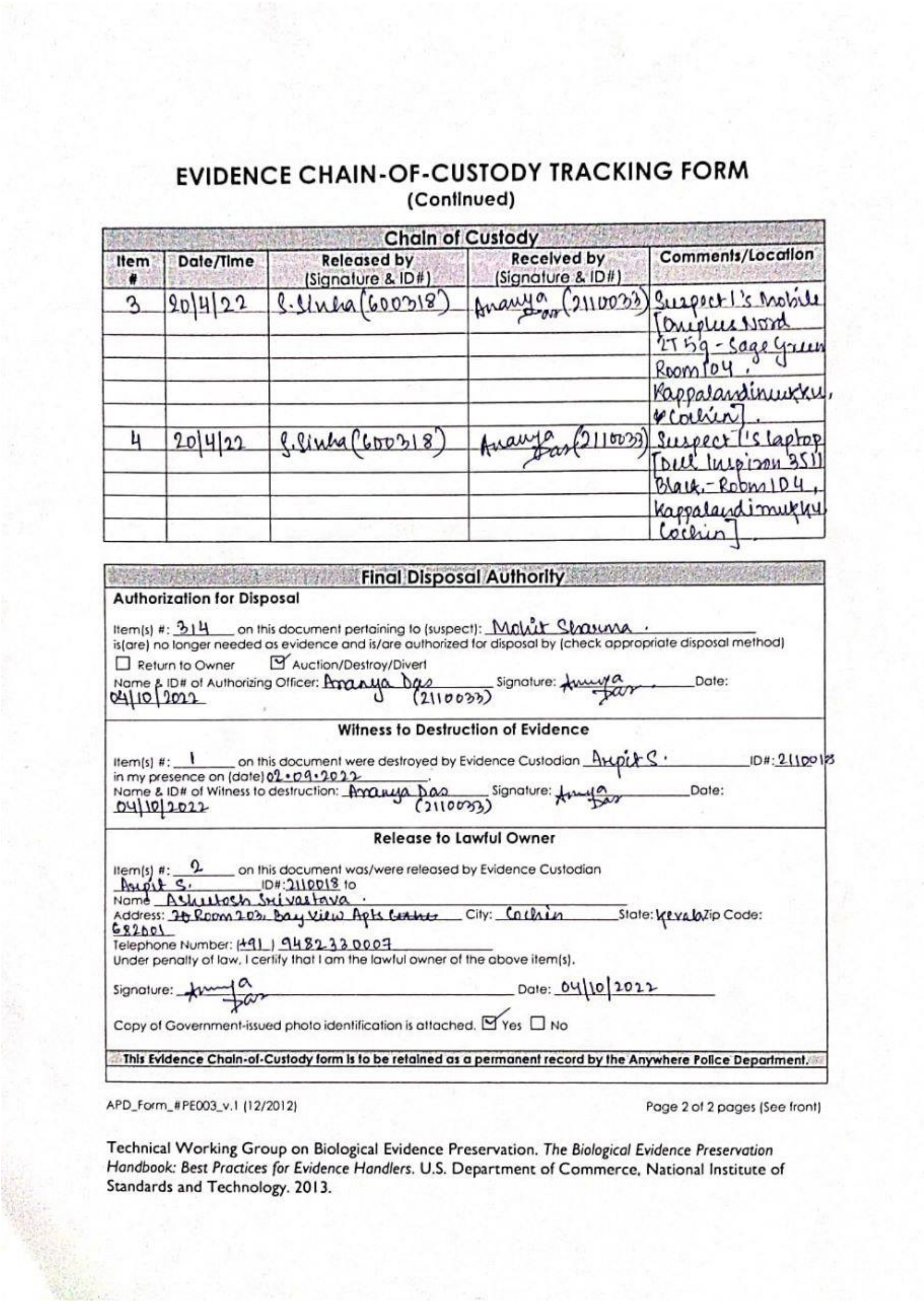
Case Number: 221·2 Offense: Murder, Cyberbullying, Impersonation
Submitting Officer: (Name/ID#) Ananya Das (2110033)
Victim: Anju Srivastava
Suspect: Mohit Sharma, Ashutosh Srivastava, Kanishka Srivastava.
Date/Time Seized: 18/04/2022, 9:27 a.m. Location of Seizure: Highway Garden Hotel (Room 342), Cochin.

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
1	1	Mobile Phone (Redmi Note 10 Pro, NN572LL/A, Amber and white, scratches on the screen cover)
2	1	Laptop (HP Pavillon x-360, 4CE460D0G, Silver, –)
3	1	Mobile Phone (Oneplus Nord 2T 5g, f1e65cf2, sage green, broken camera lens)
4	1	Laptop (Dell Inspiron 3511, 4F34DG1, Black, –)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**
1	18/4/22	T. Parekh (700352)	Ananya Das (2110033)	Victim's mobile- [Redmi Note 10 Pro (Amber) - HG Hotel, Cochin].
2	20/4/22	(536100)	Ananya Das (2110033)	Victim's laptop [HP Pavilion- x-360 - Silver. Room 203, Bay View Apartments, Cochin].

APD_Form_#PE003_v.1 (12/2012)

Page 1 of 2 pages (See back)



EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM
(Continued)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
3	20/4/22	S. Sinha (600318)	Ananya Das (2110033)	Suspect 1's Mobile
				[Oneplus Nord
				2T 5g - Sage Green
				Room 104,
				Kappalandimukku,
				Cochin].
4	20/4/22	S. Sinha (600318)	Ananya Das (2110033)	Suspect 1's laptop
				[Dell Inspiron 3511
				Black - Room 104,
				Kappalandimukku
				Cochin].

Final Disposal Authority

Authorization for Disposal

Item(s) #: 3 | 4 on this document pertaining to (suspect): Mohit Sharma.
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☑ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: Ananya Das (2110033) Signature: Ananya Das. Date: 04/10/2022

Witness to Destruction of Evidence

Item(s) #: 1 on this document were destroyed by Evidence Custodian Arpit S. ID#: 2110018
in my presence on (date) 02.09.2022.
Name & ID# of Witness to destruction: Ananya Das (2110033) Signature: Ananya Das Date: 04/10/2022

Release to Lawful Owner

Item(s) #: 2 on this document was/were released by Evidence Custodian
Arpit S. ID#: 2110018 to
Name Ashutosh Srivastava.
Address: ~~20~~ Room 203, Bay View Apts ~~Cochin~~ City: Cochin State: Kerala Zip Code: 682001
Telephone Number: (+91) 9482330007
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: Ananya Das Date: 04/10/2022

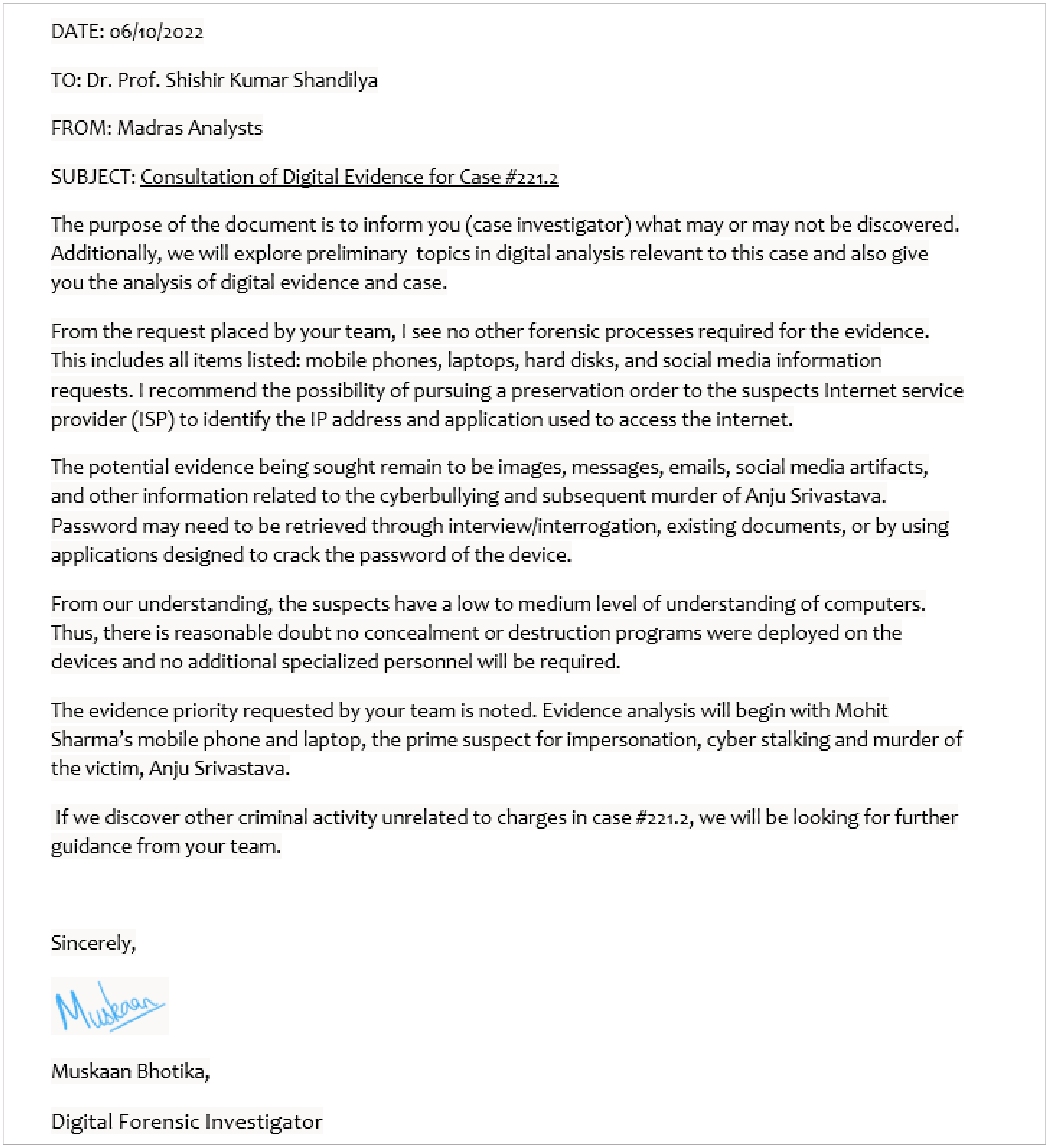
Copy of Government-issued photo identification is attached. ☑ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers.* U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

Appendix B: Consultation Letter



DATE: 06/10/2022

TO: Dr. Prof. Shishir Kumar Shandilya

FROM: Madras Analysts

SUBJECT: Consultation of Digital Evidence for Case #221.2

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 and also give you the analysis of digital evidence and case.

From the request placed by your team, I see no other forensic processes required for the evidence. This includes all items listed: mobile phones, laptops, hard disks, and social media information requests. I recommend the possibility of pursuing a preservation order to the suspects Internet service provider (ISP) to identify the IP address and application used to access the internet.

The potential evidence being sought remain to be images, messages, emails, social media artifacts, and other information related to the cyberbullying and subsequent murder of Anju Srivastava. Password may need to be retrieved through interview/interrogation, existing documents, or by using applications designed to crack the password of the device.

From our understanding, the suspects have a low to medium level of understanding of computers. Thus, there is reasonable doubt no concealment or destruction programs were deployed on the devices and no additional specialized personnel will be required.

The evidence priority requested by your team is noted. Evidence analysis will begin with Mohit Sharma's mobile phone and laptop, the prime suspect for impersonation, cyber stalking and murder of the victim, Anju Srivastava.

If we discover other criminal activity unrelated to charges in case #221.2, we will be looking for further guidance from your team.

Sincerely,

Muskaan

Muskaan Bhotika,

Digital Forensic Investigator

Appendix C: References

Facebook. (2017). *Information for Law Enforcement Authorities.* Facebook.com. Retrieved from https://www.facebook.com/safety/groups/law/guidelines/

Turvey, B.E. (2008). *Criminal Profiling: An Introduction to Behavioral Evidence Analysis.* Burlington, MA: Elsivier, Inc.