**Q1: We have evaluated the role of incident report writing. Write the major components that are necessary in the incident report writing? How do they help in the case? Discuss the tools that help you in the process and how? What role do the report do for the attorneys in the Hon. Court of justice?**

Ans:

Components and Guidelines for Writing Reports

• Hypothetical questions based on factual evidence

• Guide and support your opinion

• Can be abused and overly complex

• Opinions based on knowledge and experience

• State the facts needed to answer the question

• Don’t include any unnecessary facts

As an expert witness, you may testify to an opinion or conclusion, if four basic

conditions are met:

• Opinion, inferences, or conclusions depend on special knowledge, skills, or training

• Witness should qualify as a true expert in the field

• Witness must testify to a reasonable degree of certainty

• Experts must know facts on which their opinions are based, or they must testify to a

hypothetical question

Structure

• Abstract (summary)

• Table of contents

• Body of report

• Conclusion

• References

• Glossary

• Acknowledgements

• Appendixes

An abstract condenses the report to concentrate on the essential information

• The body consists of the introduction and discussion sections

• The conclusion starts by referring to the report’s purpose, states the main

points, draws conclusions, and possibly renders an opinion

• References and appendixes list the supporting material to which your work

refers

Importance of Reports

Communicate the results of your investigation

• Including expert opinion

• Forensic reports can:

• Provide justification for collecting more evidence

• Be used at a probable cause hearing

• Communicate expert opinion

• U.S. district courts require expert witnesses to submit written reports

• State courts are starting to also require them

• Rule 26, Federal Rules of Civil Procedure requires submission of the expert’s

written report that includes:

• Testimony is based on sufficient facts or data

• Testimony is the product of reliable principles and methods

• Witness has applied the principles and methods reliably to the facts of the case

• Written report must specify fees paid for the expert’s services

• And list all other civil or criminal cases in which the expert has testified

• Keep a copy of any deposition notice or subpoena so that you can include the

following:

• Jurisdiction

• Style of the case

• Cause number

• Date and location of the deposition

• Name of the deponent

• Deposition banks

• Examples of expert witness’ previous testimonies

Generating Report Findings with Forensics Software Tools

• Forensics tools generate reports when performing analysis

• It is still your responsibility to explain the significance of the evidence

• Report formats

• Plaintext

• Word processor

• Spreadsheet

• HTML format

Tools include:

• DataNumen for Outlook and Outlook Express

• FINALeMAIL for Outlook Express and Eudora

• Sawmill-Novell GroupWise for log analysis

• MailXaminer for multiple e-mail formatas and large data sets

• Fookes Aid4Mail and MailBag Assistant

• Paraben E-Mail Examiner

• AccessData FTK for Outlook and Outlook Express

• Ontrack Easy Recovery EmailRepair

• R-Tools R-Mail

• OfficeRecovery’s MailRecovery

MXToolBox for decoding e-mail headers

• FreeViewer with free tools for various servers

• Tools allow you to find:

• E-mail database files

• Personal e-mail files

• Offline storage files

• Log files

• Advantage of using data recovery tools

• You don’t need to know how e-mail servers and clients work to extract data from

them

After you compare e-mail logs with messages, you should verify the:

• Email account, message ID, IP address, date and time stamp to determine whether

there’s enough evidence for a warrant

• With some tools

• You can scan e-mail database files on a suspect’s Windows computer, locate any emails the suspect has deleted and restore them to their original state

All U.S. district courts and many state courts require expert witnesses to submit

written reports

• Rule 26 of the FRCP requires expert witnesses who anticipate testifying to

submit written reports

• Attorneys use deposition banks to research expert witnesses’ previous

testimony

• Reports should answer the questions you were retained to answer

• A well-defined report structure contributes to readers’ ability to understand the

information you’re communicating

• Clarity of writing is critical to a report’s success

• Convey a tone of objectivity and be detached in your observations

Q2: **We have observed that the crimes against children and women are increasing across the globe. One such case came to your light when lady was mentally harassed with morphed pictures of her. Later intimidated for ransom. The incident has mentally tortured the lady. List down the help you would offer as forensics expert to the lady. 1) for her (victim’s) safety against further crime  2) for finding the perpetrator and tracking them down 3) the laws that support the lady (In India) that she can use for punishing the offenders.**

**Ans :**

**a**)

* Keep a record of conversation as evidence

Person blackmailing you might have sent you the morphed image or had a conversation in the context of threat. These images or conversations will be supported as evidence. Record the conversation rather than just taking screenshots. In case the offender is blackmailing on a video call, screen record it. For applications like Snapchat, record it using an appropriate recording application or capture a picture of it.

In case an anonymous person is trying to blackmail you, keep conversations online. Internal data attached to the online message will help find the message’s location more quickly. Additionally, try to make conversation on messaging apps based in India. As per the police authority of the cyber cell police station, they find themselves incapable of resolving the case when the servers of social media sites are based outside India as they are out of the ambit of Indian law. This is to note that it is difficult to track the originator of the message in the case of WhatsApp.

* Do not be an easy victim

Do not engage with the blackmailers as it will backfire all the solutions. The blackmailer may sense himself/herself/themself more potent in the situation, possibly resulting in incensed demands. The blackmailer may also come up with a claim that the accuser was also active in this act and that it was consensual.

No engagement with the blackmailer also means ‘no negotiation’. Negotiating or giving in to their demands just gives offenders more power – and they are likely to use this power to make even more threats.

* File a complaint

Cybercrimes come under global jurisdiction; it means that one can file a complaint anywhere in India irrespective of your exact location. Reach out to your nearest cyber cell and report information of the blackmail to the authority present there.

One can also file an FIR in a local police station with a separate cyber cell office. If your application gets rejected, proceed to the Judicial Magistrate in the area where the application is filed.

* Online medium to file a complaint

The Ministry of Home Affairs has launched an online National Cyber Crime Reporting Portal to file a report and track all cybercrime convenience. There are two types of cases filed in the said portal: women-related cases and other crimes (related cybercrimes). The victim will have to submit information such as name, state, platform where the incident occurred, an attached document of evidence to support the allegations, information related to the suspect, etc.

Even though the portal provides the option ‘reason for the delay in reporting’ if the victim delays in reporting, it’s appropriate if the report is filed in the initial stage of blackmailing.

* Involve a lawyer expert in a cyber domain

One of the primary reasons for involving a cyber lawyer is to prevent morphed images/videos from being published. They can also put a short end to blackmail and threats.

b) Stegnography, geo location finding, Phone number and email address tracking,

using help from NIXI and ISP.

**c)** Legal provisions that safeguard you

Section 67 of the Information Technology Act, 2000

Section 67 of the Information Technology Act, 2000 imposes criminal liability on release or disclosure of any material which is inter alia lascivious or engages to the prurient interests. The punishment on the first sentence is imprisonment up to three years and with a fine of rupees five lakhs, and subsequent convictions to be punished with imprisonment up to five years and fine which may extend up to ten lakh rupees.

If the offender is a habitual offender, i.e., if the offender tries to morph and harasses again despite action against him/her, the punishment will be doubled.

Section 292 of the Indian Penal Code, 1860

According to Section 292 of the Indian Penal Code, 1860, a book, pamphlet, paper, writing, drawing, painting, representation, figure, or any other object shall be deemed obscene if it is lascivious or appeals to the prurient interest or its effect (is) such as to tend to degrade and corrupt a person.

Section 509 of IPC (Insult to the modesty of a woman)

Section 509 penalizes abusing the dignity of a woman. This Section is frequently used in consonance with other sections of IPC involving sexual assault. As per this Section, whoever intends to insult the modesty of any woman by using any word, sound, gesture, or exhibit any object, intentionally that intrudes upon the privacy of such woman is punishable.

In the case State of Punjab v. Major Singh (1996), it was held that any act done in the presence of a woman that is indicative of sex according to the common notion of mankind is covered under this Section. To be more precise in the context of the topic, any message that conveys lascivious or lustful comments upon the body of a girl and circulating the image is covered in the said Section. The punishment for the act of damaging the dignity of a woman under this Section is imprisonment up to one year, or fine, or both.

Section 499 and 500 IPC (defamation)

Defamation is one recourse a victim can take in such a situation. According to Section 499 of IPC, either creating or publishing ostensibly defamatory remarks about a person in the form of words or writing or visible representations that potentially harm a person’s reputation is culpable or punishable. Therefore, if a person is trying to harm someone’s image or reputation, it will be considered an offence and will come under this section.

The victims can also choose to take support under Section 500 of the Indian Penal Code. Section 500 of IPC provides the penalty for defamation, which can be simple imprisonment for up to two years with or without a fine.

Q3: **As an expert in cyber forensics, we have observed a change in the global cyber-crime landscape. The crime has moved on from individual doing for bragging in early 1980’s to now highly organized one backed by powerful organizations including government bodies. What has changed in last 40 years in cyber space and what according to you are the reasons for this evolution. Discuss the change in detail and their reasons.**

**Ans:**

cyberthreat has been in existence since the early stages of communication and is evolving since then with the subseing in the 1970s to cryptojacking in 2021, cybercrimes tend to become more and more sophisticated with time.

With every passing decade, the technological society and cybersecurity professionals find themselves amidst highly coordinated and relentless attacks on digital assets and infrastructure, where the existing solution or defense either fell short or was not scalable enough for the implementation of emerging technology.

The 50s ad 60s

Landline Hack: Throughout the 1950s and 60’s the wired telecommunication technology was booming, and

landlines were available in the majority of households across developed countries.

This decade also marked the onset of the first digital-based crime known as “Phreaking,” where the perpetrators exploited the tone system used in telephone networks.

The episode dates back to the late 1950s, where a group of phreaks, a short form for the term “Phone Freaks” , decided to hack telephone networks

by making unauthorized and unauthenticated long-distance phone calls by reverse-engineering the tones used by the telephone organizations.

They also set up special party lines to help other fellow phreaks. Perpetrators often impersonated officials, an extensive search of the

Bell Telephone company garbage to find any secret information or data, and experimented on the early telephone hardware to learn how to exploit them meticulously,

which results in free long-distance telephone calls.

The 70s

“The introduction of computer virus”

The decade of over-the-top fashion and new genres of music also saw a new change in the digital landscape. Though research on self-replicating programs was in progress since the ’50s, the first practical implementation, i.e., a computer virus attack was seen in the early 1970s . Bob Thomas, an engineer at BBN Technologies, wrote an experimental self-replicating program, which could move between computers connected by the ARPANET — the technical foundation of the internet .

As it could move from one system to another, it was termed as ‘Creeper,’ and while coping itself to the remote system of the 33 ASR teletype model, it left a message that read: “I’M THE CREEPER: CATCH ME IF YOU CAN,”. The techniques which were used in the Creeper were later used in the McROSS — Air traffic simulator to allow certain parts of stimulation to move across the network. The invention of Creeper was soon followed by the development of its enhanced versions. Ray Tomlinson later coded an enhanced version of the Creeper and also went on to write a program called the Reaper, which moved through the ARPANET removing the existing copies of the Creeper.

With the trend of developments and enhancements that defined this decade, programmers with malicious intent for destruction began to emerge, and soon various other viruses were coded and deployed. One of the progenies of such a trend was the rabbit virus that came to light in 1974. This virus is also considered by some as the foundation to early malware, as it was coded to self-replicate until the system crashed .

The 80s

The decade that was witness to the birth and propagation of personal computers and wireless telecommunication was also witnessing a prominent growth of destructive viruses. In the same year of 1981, when IBM released its first personal computer, a ninth-grader from Pittsburgh wrote a program called “Elk Cloner” that attached itself to Apple DOS 3.3 OS and was designed to be activated on its 50th use. This was the first virus to appear in the wild and was spread through the mean of the floppy disk.

The term ‘Computer Virus’ was coined by Leonard Adleman, and research termed “Computer Viruses – Theory and Experiments” was first published by his student Fred Cohen in 1984. With the passing years and constant evolution of technologies, viruses started becoming more sophisticated and destructive every year. In 1986, the PC platform was struck with the first-ever “Global epidemic” called the “brain virus,” as the internet was connecting many systems across the globe, hence, scaling up the spread of the virus. The propagation of the brin virus depicted the lack of security of the systems and was followed by the Vienna virus in the 1987’s, the first-ever virus which was meant to destroy the data.

This decade saw the actual rapid evolution of computer viruses that began to be classified into different categories based on their behavior, such as worms, trojans, etc., that developed with time. The first-ever worm— Morris Worm, was released in November 1988 by Robert Tappan Morris. Morris wasn’t aware of his creation as to what capabilities it held, as it was not designed with an intent of malice. In 1988, the Morris worm, which replicated itself soon with time, evolved into the world’s first large-scale Denial-Of-Service (DOS) attack. It spread through the world and brought many organizational servers and personal computers to a halt. Though Morris released the solution soon enough, for shutting down the program, severe damage caused by the worm was already done and evident. Morris was prosecuted and charged with violating the Computer Fraud and Abuse Act in 1989 .

Ransomware attacks first became known to the public in 1989, where the “Aids Trojan” was used to hide files. It was written by Joseph Popp and coded so that the files were encrypted with their names and, when done, displayed a message that stated: “User license to use the software has been expired.” The victims were asked to pay 189 dollars to the PC Cyborg Corporation to receive the repair tool that decrypted the encrypted files . Though this was not considered extremely damaging as encrypting files with names backfired and was easy to restore, this gave rise to the idea of extortion through encryption which soon caught on. Since then, ransomware attacks have evolved and have become more sophisticated, as seen in recent times. Ransomware has grown to be the biggest cyberthreat in today’s time.

On the positive side, this decade witnessed the rise of cybersecurity, with many antivirus products becoming commercially available in the market. Many businesses targeting this market emerged around this period, which includes renowned cybersecurity giants such as Avast, McAfee, etc.

The 90s

As the world went online through the boom of the internet, this decade witnessed the first polymorphic viruses that replicated themselves while the original algorithm was intact in order to avoid any kind of detection.

As organizations began to digitalize and incorporated this into their marketing strategy, i.e., providing free disk, this gave malware a platform to spread further. By 1996 many viruses evolved like the stealth capability, polymorphic viruses, macro viruses, etc. They kept multiplying and spreading in the wild in such a way that by 2007, there were more than five million viruses and malware .

Towards the end of the 1990s, emails were a booming trend, and almost everyone with a system and internet connection possessed an email-id for themselves to communicate with ease. This became one of the most popular platforms for threat actors to spread malware and spam. Phishing attacks made the most use of this platform to trick victims into providing sensitive information or downloading malicious attachments.

In 1999, the Melissa Virus surfaced, which initiated the victim’s system via a Word document. It emailed copies of itself to the first 50 email addresses in Microsoft Outlook. It is still one of the fastest spreading viruses, which caused a damage of 80 million dollars to rectify and fix the damages.

The Turn of the Century

AS time progressed, viruses started becoming more progressive and sophisticated, which was evident throughout the 2000s. Numerous viruses came into existence, targeting specific functions of the system via the internet, network, and techniques, ranging from keystroke logging to advanced ransomware attacks.

The Distributed Denial of Service (DDOS) was the epitome of network-based attacks, as the world noticed a breakpoint in Feb 2000, where a series of DDOS attacks surfaced when a 15-year-old Canadian hacker known as the “mafia boy” mounted and executed the DDOS attacks which targeted the e-commerce websites (including Amazon and eBay). The attack led to a loss of 1.7 billion dollars and forced organizations to shut down their websites to regulate legitimate traffic flow.

With the start of the 2000s, a new era of malware emerged as emails were seen as exploitable access points for the perpetrators, who aimed at causing more destruction. The ‘ILOVEYOU’ worm infected nearly 50 million systems which corrupted the data and self-propagated itself by exploiting the victim’s email contacts. This gave an insight into how cybersecurity was crucial and the necessity for all systems to have antivirus software installed to safeguard their systems and data.

The 2000s came to be known as the carding era, where digital cash was still a new thing, and people using their Debit Credit cards to purchase various items online. With people relying on the internet for various purposes and digital transactions becoming a trend, Carding attacks increased. Speculations started with the Russian carding forums and marketplaces used by the perpetrators to steal card details and utilized sensitive information for multiple purposes like identity theft and phishing attacks. Cardholders who often used e-commerce platforms were susceptible to carding and phishing attacks, allowing perpetrators to access sensitive information critical to their personally identifiable information (PII). The stolen details were often sold to other criminals or put on sale on various hackers’ platforms and the dark web. The stolen details are often used to make new, fake cards. One such website was the CarderPlanet, founded by Golubov D.I. et al. in the year 2001.

The Twen’tē-tens

Data breaches soon became the center of attraction for the information security landscape due to the emergence of various malware attacks in the decade. In contrast to the previous era where the threat landscape saw the evolution and drastic changes occurring in the time frame of few years, the 2010s and the subsequent decade would see a change in trend every year. There were not any notable novel cyberthreats in this decade, but the development in the existing threat and attack vectors, and their aspects such as mode of dissemination, target, counter anti-cybercrime strategies contributed to the exponential growth of the threat landscape. As time passed by, various new attacks were witnessed with the bypassing years like :

The year of the data breach – 2011

The post PC era – 2012

The year of online banking threats – 2013

The year of cyberattacks – 2014

The year of botnets – 2015

The year of digital extortion – 2016

The year of global ransomware outbreaks – 2017

This decade saw numerous organizations become victims of data breaches and malware attacks. Especially the initial years were known to be the most challenging for organizations and cybersecurity professionals as the victims of data breaches lost reputation due to the loss of confidential and sensitive information and bore resulting financial burdens and losses towards stabilizing the situation and fixing the damages. Conditions were adverse where organizations like RSA and Sony Play Station had no other options other than disclosing the details and facts about the attack against their organization to assure their customers that proper mitigation steps are taken to resolve the issues.

After initial years the digital data and online presence of users started to move away from personal computers and towards mobile and virtual machines. This change is marked as the post-PC era and also noticed a significant rise in the cybercrimes focused on Android platforms, social networking sites, cloud, etc. As it took less than three years for android devices to reach the threat level of the PCs, which took nearly 14 years for the same, mobile-based cyberthreats and attacks rose in recognition.

The Twen’tē-20s

The future of cyberthreat is projected to be similar to that of the previous decade, where the existing threat vectors and attacks will be developed upon with unique implementation across emerging technologies such as the Internet of Things (IoT), cloud computing, and virtual machines, and blockchain technology. Attack vectors such as phishing and social engineering are here to stay, and the cybersecurity experts do not see them going away any time soon.

Apart from this, the IoT and blockchain technology has given rise to a new form of threat known as crypto-jacking. Crypto-jacking is an evolved form of botnet attacks and is an attack carried out by perpetrators who gain unauthorized access to the victim’s devices (PCs, Tablets, Mobiles, serves of an organization, etc.) to mine cryptocurrencies. Cryptocurrency is digital or virtual money in tokens or coins based on blockchains, and Bitcoin is one of the most popularly known cryptocurrencies. The main of crypto-jacking is to benefit from crypto mining without bearing the vast costs (mining hardware, high electricity costs) of the mining process . Cybercrimes related to cryptocurrencies are seen from 2009 till date, but the cryptocurrency sector is booming, and many individuals investing in cryptocurrencies (especially the ones that have larger values such as bitcoin) have drawn the attention of many attackers. It embeds itself on the victim’s device and uses its resources to mine cryptocurrency.

Conclusion

Cybercrimes have evolved drastically! And malicious use of programs and exploitation of vulnerabilities has greatly modified the cybersecurity landscape. From small viruses that were created as pranks to their use as a threat evolved with time and then scaled to spread across the globe with change from ARPANET to the internet. With the introduction of platforms such as email, networks, cloud, IoT, blockchain, etc. that connected people and data across the globe with lightning speed, the attackers were on the run to create the perfect virus, malware, and other attacks which would compromise on the authenticity, integrity and the confidentiality of the data and cause great harm to the victim and systems.

With the development of technology and integration of security standards, attackers pushed themselves to be a step ahead and create advanced malware, trojans, ransomware, and protocols and procedures that successfully bypassed the security mechanisms. This has been a recurring stance since the technology started developing. Cybercrimes, like cybersecurity, are a forever developing and evolving process. Perpetrators are constantly working on building sophisticated threats, malware, etc., on infiltrating the prevalent and upcoming security measures. It is essential to enhance security measures and protect ourselves from becoming a victim of the ever-growing cybercrime.

Q4: **You are approached by a Local Police body for help in a case where the person’s bank account has been debited with over 10 Lakh INR in last 24 hours. Thankfully the person has registered the complaint at the helpline 1930 and registered the complaint with the bank as well. However, the case unfolds with the person receiving a call from a reputed company for the gift/prize for being a regular customer. The person neither share the OTP nor the bank details and certainly not the credit card or internet banking details. Later on, in your investigation, it was found that the person can be either victim of card cloning or SIM card replication.           (7+3  =10 Marks)**

1. **In order to proceed the first case of card cloning, what steps do you take? List at least 7 of them.**
2. **In the later possibility of sim card replication, what steps you may take to find the mistake on the Telecom company or anyone else.  You can consider to verify with the telecom agency for the coordinates of phone usage. Apart from this, what else you should do?  List at least 2 plan of action for you.**

Ans:

step investigation procedure:-

Letter to Bank:

AOF (Account Opening Form) / Bank Account

Statement of the complainant

Detailed particulars of each banking

transaction

ATM-cum-Debit Card details of the complt.

Certificate u/s 2A of Bankers Book of Evidence

Act, 1891

Letter to Mobile Service Provider:

Subscriber Details

Date of Activation

CAF (Customer Acquisition /Application

Form)

CDR (Call Details Record) of the complainant

as well as of the accused person for the

relevant period

Certificate u/s 65B (4) (c) of Indian Evidence

Act, 1872

Letter to Online Payment Gateway:

Notice u/s 91 of Cr.P.C. to be issued

Detailed description of each fraudulent transaction with

relevant to Wallet ID?

IP details of the computer system used along with date and time

for committing the said fraudulent transaction?

Whether accused had created or registered any account in your

website for committing the offence?

Date & time of registration / creation of ID

IP details along with date & time of the computer system used

for registration/ creation of the account

Type of operating system of the computer system of the

fraudster

Physical address of the computer system

 Mobile phone numbers / E-mail addresses of the accused used for

registration or for generation of OTP or for any authentication process

 Mailing address of the accused

• Whether accused had opened any wallet in your website for

committing fraudulent transactions?

• Date and time of creation of Wallet

• IP details of the computer system used by the accused for creation of

the said wallet?

• What was the transaction limit set by the accused for the said Wallet?

• Whether the said Wallet created by the accused was linked to any bank

account?

• Details of the bank account along with the bank name and IFSC Code

may please be furnished.

• Detailed transactions made by the accused through the said Wallet

may please be furnished.

• Whether accused had purchased or made online shopping

of any goods or articles through your website?

• Counter foil receipt in respect of delivery of goods by online

shopping website to the fraudster [DRS:- Delivery Run

Sheet]

• Detailed particulars of Courier Agency or company

personnel along with his contact number or e-mail ID; who

had delivered the purchased goods / products to the

fraudster

• Date and time of delivery of goods

• Address of delivery of goods

• As these are fraudulent transactions, it is hence requested to

kindly initiate the process for revert back of the defrauded

amount to the bank account of the complainant.

• Certificate u/s 65B (4) (c ) of Indian Evidence Act, 1872

Letter to E-mail Service Provider:

Notice u/s 91 of Cr.P.C. to be issued

o Account Registration Details of the e-mail account

o Log Details

o Mobile Phone Number used at the time of registration and

updation of the e-mail account {registered mobile phone

number}

o Secondary e-mail account

o Certificate u/s 65B (4) (c) of Indian Evidence Act, 1872

Letter to Internet Service Provider:

End user details of IP Addresses

CAF / NTC in respect of the user subscriber in

respect of the alleged IP address

 Other relevant information in respect of the

user subscriber that is the address of

correspondence, contact number, e-mail IDs

and billing details

MAC ID of the alleged computer system / IMEI

address of the computer resources with respect

of the relevant IP address.

Certificate u/s 65B of Indian Evidence Act, 1872

Letter to Bank:

Detailed information as regards of the account holder in

respect of the bank account of the accused:-

• Name of the account holder

• Correspondence address of the account holder

• Contact number

• Registered Mobile Number

• E-mail account if any

• Date of opening of bank account

• Original Account Opening Form {AOF} in respect of the

aforesaid bank account.

Letter to Bank:

• Original documents submitted by the account holder at the

time of opening of the account, in compliance to the

provisions of KYC norm.

• Account statement in respect of the aforementioned bank

account for the period from \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

• Present status of the aforementioned bank account

• Whether ATM-cum-Debit card has been issued to the

Customer by the Bank?

• Card Number

• Date of submission of application by the accused for issuing of

ATM-cum-Debit card

• Date of issue

• Place of issue {on which address ATM Card was delivered to the

customer}

• Application submitted by the accused in the bank to provide ATMcum-Debit card

• To freeze the operation of the bank account.

• On which date the said bank account has been

frozen.

• Amount frozen may please be furnished.

• Whether the said bank account of the accused is

being involved in any of the offence? If involved,

kindly furnish the documents pertaining to the said

aspect and the action taken by your bank into the

said matter.

• Certificate u/s 2A of Bankers Book Evidence Act, 1891

may kindly be furnished along with the report.

B)Immediately contact the service provider immediately, in case you find that your mobile number is inactive or out of range for long time. Take back the control of your mobile number, with changed password.

Verify and change or reset the passwords and PIN numbers of your sensitive financial accounts and social media accounts.

Check your financial statements like credit/debit card, bank, payment apps and other financial accounts for any unauthorized charges/changes. Immediately report about any changes or charges to respective authorities.

In case of a SIM fraud, contact phone banking immediately to have your account blocked and avoid further fraud. Latter submit your identity documents by writing the proper reason and sign for getting the new SIM.

Check for any authorized posts or activity on your personal or social media accounts. In case you notice any such posts take corrective steps and inform the social media help Centre to regain control of hacked account.

Q5: **One of the important information related to the case is residing in the email of the accused. The cyber forensic expert looks for it in the hard disc image but where should he/she look? Discuss at least 5 possible plan of action for the expert where forensic expert must search for evidence in this case.**

**Ans:**

* Examining Email Messages:

Since the crime is committed via e-mail, I would first access the victim’s computer to recover the evidence. Using the victim’s e-mail client, I would find and copy any potential evidence. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders. If I can’t actually sit down at the victim’s computer, I will guide the victim on the phone to open and print a copy of an offending message, including the header. The header contains unique identifying numbers, such as the IP address of the server that sent the message. This information helps me trace the e-mail to the suspect.

* Copying an Email Message:

Before I start an e-mail investigation, I will copy and print the e-mail involved in the crime or policy violation. I will also want to forward the message as an attachment to another e-mail address, depending on my organization’s guidelines. The following activity shows how to use Outlook 2007, included with Microsoft Office, to copy an e-mail message to a USB drive.

1. Insert a USB drive into a USB port.

2. Open Windows Explorer or the Computer window, navigate to the USB drive, and leave this window open.

3. Start Outlook by clicking Start, pointing to All Programs, pointing to Microsoft Office, and clicking Microsoft Office Outlook 2007.

4. In the Mail Folders pane, click the folder containing the message I want to copy. For example, click the Inbox folder. A list of messages in that folder is displayed in the pane in the middle. Click the message I want to copy.

5. Resize the Outlook window so that I can see the message I need to copy and the USB drive icon in Windows Explorer or the Computer window.

6. Drag the message from the Outlook window to the USB drive icon in Windows Explorer or the Computer window.

7. Click File, Print from the Outlook menu to open the Print dialog box. After printing the e-mail so that I have a copy to include in my final report, exit Outlook.

* Viewing Email Headers:

After I copy and print a message, I will use the e-mail program that created it to find the e-mail header. After I open e-mail headers, copy and paste them into a text document so that I can read them with a text editor such as a Notepad.

To retrieve an Outlook e-mail header, I would follow these steps:

Start Outlook, and then select the original of the message I copied as mentioned above.

Right-click the message and click Message Options to open the Message Options dialog box. The Internet headers text box at the bottom contains the message header

Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.

Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.

Save the document as Outlook Header.txt in my work folder. Then close the document and exit Outlook.

* Examining Email Headers:

The next step is examining the e-mail header I saved to gather information about the e-mail and track the suspect to the e-mail’s originating location. The primary piece of information looking for is the originating e-mail’s domain address or an IP address. Other helpful information includes the date and time the message was sent, filenames of any attachments, and unique message number, if it’s supplied.

To open and examine an e-mail header, follow these steps:

1. Open the Computer window or Windows Explorer and navigate to my work folder.

2. Double-click a .txt file containing message header text, such as Outlook Header.txt. The message header opens in Notepad.

The e-mail header provides a lot of information. Lines 1 to 5 show the e-mail servers through which the message traveled. Line 1 shows the return path, which is the address an e-mail program uses for sending a reply, usually indicated as the “Reply to” field in an e-mail. Do not rely on the return path to reveal the e-mail’s source account, however. Spoofing (faking) an e-mail address in the Return-

* Examining Additional Email Files

E-mail programs save messages on the client computer or leave them on the server. How e-mails are stored depends on settings on the client and server. On the client computer, you could save all your e-mail in a separate folder for record-keeping purposes. For example, in Outlook, you can save sent, draft, deleted, and received e-mails in a .pst file, or you can save offline files in an .ost file. With these client files (.pst and .ost), users can access and read their e-mail offline (when their computers aren’t connected to the central e-mail server).

In Web-based e-mail, messages are displayed and saved as Web pages in the browser’s cache folders. Many Web-based e-mail providers also offer instant messaging (IM) services that can save message contents in proprietary and nonproprietary file formats. These files are usually stored in different folders than Internet data files are. For example, in Windows, you can scan IM files and folders under Documents and Settings\username\Application Data or under Program Files.

* Tracing an email message:

As part of the investigation, I will determine an e-mail’s origin by further examining the header with one of many free Internet tools. Determining message origin is referred to as “tracing.” I would several sources such as DNS Registry, ARIN to find out the domain thats hosting the email server and try trace the email to a specific end-point.

Using Network Email Logs:

Network administrators maintain logs of the inbound and outbound traffic routers handle. Routers have rules to allow or deny traffic based on source or destination IP address. In most cases, a router is set up to track all traffic flowing through its ports. Using these logs, one can determine the path a transmitted e-mail has taken. The network administrator who manages routers can supply the log files you need. Review the router logs to find the victim’s (recipient’s) e-mail, and look for the unique ID number

Network administrators also maintain logs for firewalls that filter Internet traffic; these logs can help verify whether an e-mail message passed through the firewall. Firewalls, such as WatchGuard, Cisco Pix, and Check Point, maintain log files that track Internet traffic destined for other networks or the network the firewall is protecting. When the network administrator provides firewall log files, you can open them in a text editor, such as Notepad in Windows or vi in UNIX.

Examining Email Server Logs:

The files that provide helpful information are log files and configuration files. Sendmail creates a number of files on the server to track and maintain the e-mail service. The first one to check is /etc/sendmail.cf, which contains configuration information for Sendmail, so you can determine where log files are stored. Sendmail refers to the sendmail.cf file to find out what to do with an e-mail after it’s received. For example, if the server receives an e-mail from an unsolicited site, a line in the sendmail.cf file can tell the Sendmail server to discard it.

Similar to the sendmail.cf file, the syslogd file includes e-mail logging instructions. By viewing this file, you can determine how Sendmail is set up to log e-mail events and which events are logged. The syslogd file’s configuration is located in /etc/syslog.conf, which contains three pieces of information that tell you what happened to an e-mail when it was logged: the event, the priority level of concern, and the action taken when it was logged. By default, Sendmail can display an event message, log the event message to a log file, or send an event message to a remote log host.

The syslog.conf file simply specifies where to save different types of e-mail log files. The first log file it configures is /var/log/maillog, which usually contains a record of Simple Mail Transfer Protocol (SMTP) communication between servers. Typically, UNIX systems are set to store log files in the /var/log directory. However, an administrator can change the log location, especially when an e-mail service specifies a different location. If you’re examining a UNIX computer and don’t find the e-mail logs in /var/log, you can use the find or locate command to find them.

* Email Forensics Tools

For many e-mail investigations, I can rely on e-mail message files, e-mail headers, and e-mail server log files. However, if I can’t find an e-mail administrator willing to help with the investigation, or if I encounter a highly customized e-mail environment, I can use data recovery tools and forensics tools designed to recover e-mail files. The following tools are specifically created for e-mail recovery, including recovering deleted attachments from a hard drive:

• DataNumen for Outlook and Outlook Express

• FINALeMAIL for Outlook Express and Eudora

• Sawmill-GroupWise for log analysis

• DBXtract for Outlook Express

• Fookes Aid4Mail and MailBag Assistant for Outlook, Thunderbird, and Eudora

• Paraben E-Mail Examiner, configured to recover several e-mail formats

• AccessData FTK for Outlook and Outlook Express

• Ontrack Easy Recovery EmailRepair for Outlook and Outlook Express

• R-Tools R-Mail for Outlook and Outlook Express

• OfficeRecovery’s MailRecovery for Outlook, Outlook Express, Exchange, Exchange Server, and IBM LotusNotes

Few vendors have products for analyzing e-mail in systems other than Microsoft, such as Apple Mail or Novell Evolution. In this section, you learn about a method for acquiring Evolution e-mail directories and extracting messages with Hex Workshop. These techniques can be used with all e-mail systems that create flat plaintext files, known as an mbox format, to store messages. Vendor-unique e-mail file systems, such as Microsoft .pst or .ost, typically use Multipurpose Internet Mail Extensions (MIME) formatting, which can be difficult to read with a text or hexadecimal editor.

To carve e-mail messages from Evolution, you need to copy the .evolution directory, its subdirectories, and content to another storage medium that can be transported to your forensic workstation. One way is to export the .evolution directory and subdirectories from an image file to a target directory by using a forensics tool, such as FTK, EnCase, X-Ways Forensics, or Sleuth Kit and Autopsy. These tools export the directory with all subdirectories to the target drive path you designate. For an e-mail recovery that requires extracting only e-mail data from a litigant’s computer, the UNIX/Linux tar command is an easy tool to use. You can create a tarball of the entire .evolution directory and uncompress it so that a hexadecimal editor on any OS can read it. For other e-mail applications that use the mbox format, a hexadecimal editor can be used to carve messages manually. This technique requires perseverance because it’s tedious and time consuming.

* Recovering Outlook Files:

I might need to reconstruct .pst files and messages. With many advanced computer forensics tools, such as X-Ways Forensics, AccessData FTK, and Guidance Software EnCase, deleted .pst files can be partially or completely recovered. Typically, additional effort is required to reconstruct these recovered files so that their content can be extracted as part of a data recovery or forensics examination. The Scanpst.exe recovery tool comes with Microsoft Office and can repair .ost files as well as .pst files. Several other recovery tools are designed to reconstruct e-mail data in Outlook and other e-mail formats. One tool that has been well tested is Advanced Outlook Repair

* Action taken:

One advantage of using data recovery tools is that I don’t need to know how the e-mail server or e-mail client operates to extract data from these computers. Data recovery tools do the work and allow me to view evidence on the computer. After I compare e-mail logs with the messages, I should verify the e-mail account, message ID, IP address, and date and time stamp to determine whether there’s enough evidence for a warrant. If so, I can obtain and serve a warrant for the suspect’s computer equipment.

Q6: **What recommendations do you give for your 12 years’ cousin who is handling the mobile phone for the first time? Give Three recommendations with proper justification. Your advice would help him use the device in judicious manner.**

**Ans:**

1. Privacy should be maintained – explain how
2. Downloading from trusted sources – explain the problems if downloads are done from unauthorised sources
3. Clicking on links, browsing safe content etc.