DATE 25 | 01 | 2022 Tuesday

Digital Forensics
Assignment

Suhan. B. Revankar
PES2UG19CS412
G Section.

CASE 1 :

As a complainant i would hand-over all digital evidences of communication between me & the culprit, like handing over accounts i.e social media account details/ creds that i used to have conversation with culprit. And my bank statements which had transaction details of INR 12.5 million transfer which i did as a result of constant blackmailing that one of the girl committed suicide & accused also sent fake copies of letters from CBI etc which is also a crime.

As investigator, i would go through all the e-mails, message exchanges between the complainant & the accused. A background check of the complainant regarding his place of stay, previous criminal records, cases etc. Also verify his statements going through his location history, mail history, calls etc. Then verify if the accuse really exist her identity, how they got into contact with each other, place where accuse stay, background check of accuse. Verify the letters sent from CBI, High court. And the statement given by accused regarding suicide of girl is true or not. Then trace the money that was transfered to the accused from the complainant, get the accused bank details, using that get the related aadhar/ proof-of-address and the phone-number. Enquire the accused by location tracking.

DATE

CASE 2 :

As an complainant, i would first register my complaint with the cyber crime department, show them the web-site, show them the calls i received & the phone-number i received it from, tell them with few of my prime suspects, provide call-recording that i received after being posted on those website if available.

As a investigator, i would first login to those website where profiles were uploaded, contact the web page admin if its a pvt company and access the logs of the website to search for the account that posted these profiles Using the account, the messages to identify IP address. Then identify the ISP to provide details of computer with IP address at the time message were posted. As a result get details of the person who did this uploading work, If the culprit used his 'home' network, he/she could be easily identified as all details would be provided by the ISP.

But if generally these type of work will be done using public networks like public wifi, cyber cafe, rail wifi etc. In those case public wifi usually has phone number based otp-authentication Therefore using phone-number culprit can be held. Cyber cafe holds the details as proof of identity of person who is using service using that person can be held. Location tracking can be done if we get access to phone number: if phone number not available using proof of identity, trace culprit home, investigate neighbours etc to get held of the culprit.

DATE

CASE 3 :

As a complainant, I would file a formal complaint explaining the scenario like what was tampered, when did we (the company) get to know abt this breach of sourse code had happend. The company's prime suspects or whom the company has doubt on. Provide the acces of system-logs, Network logs etc to the investigation team. Also provide the details of my primary suspect

As a investigator, i would visit the complainant's premises & scan, make a copy of logs of e-mail, system logs, network logs etc. Identify all the requests, responses, e-mails, packets that was directed from the company's private home network to the public network / outside the company network (as usually this would not happen in company, as all will be done within the company's pvt network). If such logs found, identify the IP addresses of those source & destination devices. Using this trace the ISP & address of place where the data has been sent. Then investigate the system where the data was sent, seize the receiver system get a complete copy, backup of the system for further investigation & to pose as an evidence, get a detailed investigation of this system done, to verify that this system has actually received those tampered files / has been done by it.

If any evidence is found against the received device owner further legal, judiciary measures can be taken against the owner of device

*****

PES UNIVERSITY