Case Type	Financial Fraud Case
Environment	Attacker hacked net banking and siphoned 60,000.00 Rupees. The case is a net banking account hacking and theft.
Industry	Union Bank (Finance Industry)
Method / Appliance Involved	Brute force password hacking Phishing and Spam mail Keylogging SIM card cloning through the use of a mobile phone
Method of Discovery	Followed the process of digital forensics by gathering information that can be related to the case. Initially the victim reported to the police that the money present in his bank account was incorrect. Company then presented a log of his transaction. This was when the anomaly was discovered. Found out that the victim got the SMS message which was sent from the Union Bank main server. Also checked the spam mail that the victim received.
Method of Solving the Problem	Investigators then searched the main server for the record that held the victim's userID and IP address which was spoofed by the attacker. Time and date were also logged so that CCTV images can be collected from where the attacker withdraws the money. Investigators identified the IP address of the device from where the actual fund was transferred, investigators came to know that the internet is accessed from the phone, and we traced down the location to Agra Railway station. Fraudster used a different mobile phone to access the internet having no call records.

Reference:

Lokhande, P. S., & Meshram, B. B. (2020, May 2). *Collecting digital evidence: Internet banking fraud - case study*. International Research Journal of Engineering and Technology. Retrieved September 20, 2022, from https://www.researchgate.net/publication/280154009_Collecting_Digital_Evidence_Internet_Banking_Fraud-Case_study

Case Type	Criminal Case
Environment	Illegal Immigrant living in the United Kingdom (possible terrorist)
Industry	Bombing / Explosives (criminal is an engineer)
Method / Appliance Involved	Used the Internet to search for information on how to make detonators and explosives.
Method of Discovery	Investigators were looking for illegal immigrants living in UK and Krenar Lusha was one of them. An investigation was then held to further scrutinize and figure out information about Krenar Lusha and as a result of analyzing internet search patterns, investigators discovered that Krenar Lusha downloaded a substantial amount of information on how to make detonators, explosives and search belts from the internet.
Method of Solving the Problem	Internet search pattern analysis led to Krenar Lusha's arrest. Furthermore, when the police received their search warrant for his apartment, they managed to find him in the process of downloading video films called "The Hezbollah Military Instructions Manual and Mobile Detonators". Authorities also found copious amounts of petrol bomb components (71.8 Liters of petrol), firearm ammunition, 14 cell phones (to be used for detonating explosive devices) and computer documents called "Ragnar's Detonators" and "The Bomb Book". It was found that he had also corresponded with people on the internet and posed as a terrorist who had ill intentions toward Jewish people and Americans.

Reference:

Krenar Lusha. prezi.com. (n.d.). Retrieved September 20, 2022, from https://prezi.com/p/rhnyc1m-q9sr/krenar-lusha/?fallback=1

Case Type	Business Case / Financial Fraud / Internal Corporate Fraud
Environment	Complex Multi-Location Network and Desktops
Industry	Banking
Method / Appliance Involved	Examination of desktop and network systems used by suspected employees.
Method of Discovery	GDF (Global Digital Forensics) focused its initial examination on particular desktop and network systems used by the suspect employees. Its examiners performed digital forensic analyses on those systems while simultaneously examining data supplied directly from the Bank's IT department regarding internal network and Internet related activity of those suspect employees. Through those examinations, GDF created lists of particular areas of interest based upon the issues related to the overall investigation and catalogued those lists to further detail certain documents and fragments of data referencing suspicious Internet activity. Using that collected information, the accounting firm was able to corroborate particular aspects of their investigation to conclude that certain Bank officers did in fact do what they were suspected of doing from the beginning. Moreover, GDF also uncovered certain activities of the suspect employees that the auditors did not suspect, but which nevertheless, played an important role in the overall investigation and the final outcome.
Method of Solving the Problem	The Auditing Committee, together with the Bank's Board of Directors, was able to terminate the accused employees and also to negotiate settlement agreements favorable to the Bank with those employees, including reducing certain benefits and severance packages owed to them under pre-existing employment agreements. In the end, the Bank saved an enormous amount of money and time by having the digital evidence to use in finalizing the issues related to the investigation and was able to make important deadlines with regards to certain SEC filings.

Reference:

Case study. Business Case Study: Internal Corporate Fraud | Computer Forensics | eDiscovery | Cyber Incident Response | Cyber Security | Computer Forensics Experts. (n.d.). Retrieved September 20, 2022, from https://evestigate.com/case-study/business-case-study-internal-corporate-fraud/

Case Type	Intellectual Property Case
Environment	Large Network, International WAN
Industry	Manufacturing/Wholesale
Method / Appliance Involved	The usage of emails to email customer contact database, financial and proprietary information to their home computer in an attempt to steal this information as they left this certain company.
Method of Discovery	These ex-employees believed that these emails were untraceable because they deleted them. GDF worked on searching the mail servers that received the information, including the database itself, they were able to extract relevant data from these servers. The desktop systems used by the former employees were forensically analyzed and the original emails were extracted. By correlating the dates and times from several sources and a review of the email and data it GDF could prove that the employees did in fact transfer the information and that the other company knew of the transfer at very high levels.
Method of Solving the Problem	The attorneys could, using the data GDF rebuilt, not only verify their suspicions and validate their conclusions, but damages, originally estimated at 65-75 Million were determined to be well over 150 million. The law firm now uses GDF to analyze and build Electronic Data Discovery requests, work depositions and handle the correlation of all aspects of their electronic data Discovery. GDF then reconstructed the raw data, defined a statistically significant corpus of data and ran the necessary reports to quantify damages.

Reference:

Case study. Intellectual Property - Garments | Computer Forensics | eDiscovery | Cyber Incident Response | Cyber Security | Computer Forensics Experts. (n.d.). Retrieved September 20, 2022, from https://evestigate.com/case-study/intellectual-property-garments/

Case Type	Drug Case
Environment	On-Site Seizure at Several Locations Throughout the United States and Canada
Industry	Pharmaceutical
Method / Appliance Involved	Systems Involved – Desktops, Laptops, E-mail, Handheld Devices and Email
Method of Discovery	A Pharmaceutical Company began receiving complaints from its representatives in certain geographical areas that sales of normally high-volume drugs were slowing down considerably. The company's internal security department as well as the security departments of its major distributors began an investigation. The results of the investigations led the security professionals to believe a significant amount of the company's product was being diverted from foreign countries into The United States and sold through smaller distributors who specialized in sales to locally, privately owned, pharmacies and dispensaries within nursing homes. The diversion activities were immediately reported to the local authorities in the regions as well as to the FDA.
Method of Solving the Problem	The attorneys could, using the data GDF rebuilt, not only verify their suspicions and validate their conclusions, but damages, originally estimated at 65-75 Million were determined to be well over 150 million. GDF then reconstructed the raw data, defined a statistically significant corpus of data and ran the necessary reports to quantify damages. GDF Computer Forensic Specialists were able to decrypt and extract a wealth of information from the systems that were forensically analyzed. By conducting a complete computer forensic analysis of all the data the hard disks contained, GDF was able to provide documentation proving drug diversions. The computer forensic analysis also showed that the distributor had purchased equipment to unwrap the foreign drugs as well as repackaging equipment, all signs of a legitimate drug repackaging and exporting company.

Reference:

Case study. Drug Diversion | Computer Forensics | eDiscovery | Cyber Incident Response | Cyber Security | Computer Forensics Experts. (n.d.). Retrieved September 20, 2022, from https://evestigate.com/case-study/drug-diversion/