Charles Sturt University

IT Masters
itmasters.edu.au

ITE513 FORENSIC INVESTIGATION

Q & A Tutorial 6

Charles Sturt University

IT Masters
itmasters.edu.au

Discussion Points

You are a detective, ands have been asked to investigate a website suspected of selling counterfeit Microsoft and Adobe applications. What would you do to find out about the website and document the content and website statistics for your investigation report?

Initial Research and Analysis:

Start by conducting initial research about counterfeit software and the legal implications of selling such products. Understand the trademarks and copyrights associated with Microsoft and Adobe products. Familiarize yourself with common indicators of counterfeit websites.

Charles Sturt University

IT Masters
itmasters.edu.au

3

Discussion Points

Obtain a Warrant (if required):

If legally necessary, obtain a warrant or court order that grants you permission to investigate the suspected website. This step may involve coordinating with legal authorities in another jurisdiction.

Technical Analysis:

Gather information about the suspected website's domain name, hosting provider, and IP address. Use tools like WHOIS lookup services and domain registration databases to identify the website owner and host.

Charles Sturt University

IT Masters
itmasters.edu.au

4

Discussion Points

Website Content Analysis:

Visit the suspected website using a secure and anonymous connection to avoid leaving traces. Take screenshots or record videos of the website's main page, product listings, descriptions, prices, and any promotional material related to Microsoft and Adobe products.

Check for Trust Signals:

Evaluate the website for any trust signals that legitimate e-commerce sites usually display, such as SSL certificates, contact information, customer reviews, and clear terms and conditions. Note any inconsistencies or suspicious elements.

Discussion Points

Investigate Product Listings:

Examine the product listings in detail. Document the names of the counterfeit software products being sold, their descriptions, prices, and any claims made about their authenticity.

Inspect Payment Methods:

If possible, proceed with a mock purchase (without completing the transaction) to understand the payment methods and any redirection to third-party payment platforms. This will help uncover any potential payment-related fraudulent activities.

Discussion Points

Capture Website Statistics:

Use web analysis tools and techniques to gather statistics about the website's traffic, visitors, and engagement. This information can be helpful in establishing the website's reach and potential impact.

Screenshot and Document Evidence:

Take screenshots or record videos of each step of your investigation. These visual records will serve as concrete evidence for your investigation report.

Record Domain Ownership and Hosting Details:

Document the domain registrar, domain expiration date, hosting provider, and hosting server location. These details can be crucial for further legal actions.

Discussion Points

Monitor Online Discussions:

Search for online forums, social media platforms, or other communities where individuals might discuss the suspected website. Gather any information, reviews, or complaints related to the website and its products.

Contact Microsoft and Adobe:

Reach out to representatives from Microsoft and Adobe to inform them about the suspected counterfeit products being sold. They might be able to provide insights or assistance in the investigation.

Discussion Points

Collate Information in a Report:

Compile all the gathered information, screenshots, videos, and analysis into a detailed investigation report. Clearly state your findings, document any potential legal violations, and suggest further actions.

Legal Action and Collaboration:

Depending on the severity of the counterfeit operations, work with legal authorities and relevant organizations to take appropriate legal action against the website owner and those involved.

Investigating online activities requires a balance between thorough investigation and respecting privacy and legal boundaries. Always consult with legal experts and follow proper protocols throughout the process.

Discussion Points

There is a benefit to investigators to have access to geotags and other geolocational information to locate and apprehend suspects and convicted criminals. Conversely, the availability of this information puts many individuals in danger of being stalked or robbed. Is greater public awareness more important than the digital evidence that it provides investigators?

- The balance between privacy and security is a complex and ongoing debate in our increasingly digital world. This issue highlights the tension between the benefits of using geotags and other geolocation data for law enforcement purposes and the potential risks to individual privacy and safety.

Discussion Points

Benefits of Geolocation Data for Investigators:

- **Crime Solving:** Geolocation data can be a valuable tool for law enforcement in solving crimes. It can help establish the movements and whereabouts of suspects or individuals of interest during specific times, aiding in establishing alibis or identifying potential connections to crime scenes.
- **Evidence Collection:** Geotags and location data from devices like smartphones can serve as digital evidence that corroborates or refutes alibis, establishes timelines, and links individuals to specific locations, which can be crucial in investigations.
- **Public Safety:** The ability to track individuals can help law enforcement respond more quickly to emergencies, locate missing persons, and prevent crimes in progress.

Discussion Points

Privacy Risks & Concerns:

- **Stalking and Harassment:** The availability of geolocation data can be exploited by malicious actors for stalking, harassment, or other harmful activities. Personal information can fall into the wrong hands, putting individuals at risk.
- **Surveillance and Abuse of Power:** Widespread access to geolocation data raises concerns about government surveillance and potential abuse of power, where citizens' movements and activities could be tracked without appropriate oversight.
- **Data Breaches:** Storing and accessing geolocation data comes with the risk of data breaches, potentially exposing sensitive information to cybercriminals.

Discussion Points

Striking a Balance:

- **Transparency and Consent:** One way to address these concerns is by ensuring that individuals are aware of when and how their geolocation data is being collected and used. Obtaining informed consent for data collection can empower individuals to make informed choices about sharing their location information.

- **Strong Legal Framework:** It's important to establish clear laws and regulations governing the collection, storage, and use of geolocation data by both private companies and government agencies. This framework should include strict safeguards to prevent abuse.

13

Discussion Points

- **Encryption and Anonymization:** Utilizing encryption and anonymization techniques can help protect individuals' geolocation data, making it more difficult for unauthorized parties to access or abuse the information.

- **Educational Efforts:** Promoting public awareness about the risks and benefits of geolocation data can empower individuals to take steps to protect their privacy, such as adjusting their device settings or using privacy-enhancing tools.

14

Discussion Points

- Both greater public awareness and the use of geolocation data for investigations are important.
- Striking the right balance requires careful consideration of the potential benefits to law enforcement and public safety, alongside robust measures to protect individual privacy and mitigate potential risks.
- Requires ongoing dialogue between technology companies, policymakers, law enforcement agencies, and civil society to ensure that the rights and safety of individuals are respected while still allowing for effective law enforcement practices.