# Criminal Profiling and Evidence Gathering with Website and Domain Name Monitoring Tools

Posted on December 25, 2019

Cybercrime is a major threat to all sectors of the community, including government institutions, businesses, and non-profit organizations. It continuously hurts the global economy by sucking up billions of dollars each year, prompting the head of the U.K.'s Government Communications Headquarters (GCHQ) to declare that fighting cybercrime should be accorded the same priority as fighting terrorism.

But is it really possible to "fight" cybercrime? Some security experts have long ceded and started focusing on cyber-resilience (the ability to bounce back after a cyber attack) instead of cybersecurity (the prevention of a cyber attack). Aside from business continuity, part of cyber-resiliency should be the legal ramifications that the victim must set in motion against the attacker. Herein lies a big challenge — discovering who the cybercriminals are.

The fact that investigators find it challenging to unmask the people behind a cybercrime has given attackers more confidence. As more and more cybersecurity solutions are developed to counter them, cybercriminals always seem to be finding new methods to get around the said solutions because they believe they can't be caught.

In this article, let's examine the profile of cybercriminals and their targets, as well as briefly illustrate how domain research and threat intelligence tools such as Website Screenshot API and Reverse WHOIS Search can help investigators identify attackers.

## Unmasking Criminals and Understanding their Targets

Cybercriminals often fall into the following categories:

- Internet activists, also known as “hacktivists,” who are motivated by political or social agenda;
- State-sponsored actors who attack the digital territory of a country on behalf of anothernation;
- Criminal groups or individuals who are in it for the money.

Who are they after? According to research, 43% of cyber attacks target small businesses, although large corporations are not exempted.

Indeed, attackers don’t discriminate between small businesses and Forbes-100 listers or government agencies and regular citizens. As long as they see gaps in a system or network, they consider these as wide open doors that allow them to launch attacks.

## How to Proceed with Criminal Profiling

Since the identifying of cybercriminals is often tricky, what investigators do is developing criminal profiles based on suspects. The process is similar to non-digital criminal investigations. Investigators collect evidence from the crime scene in the hope of assembling and analyzing them to get an idea of who the suspects are.

Have they committed this crime before? What are their motives? Who are they? Investigators aim to answer these questions as they gather evidence both physically and virtually.

But instead of analyzing an attacker’s emotional, mental, and physical characteristics, cybercrime investigators look for any of these data components that can point them to the domain (and eventually the person) responsible for the attack:

- **IP addresses and WHOIS records:** IP addresses are particularly helpful as investigators can easily do a WHOIS search to get all the registration details from their WHOIS records. Investigators can then perform a reverse WHOIS search by using any of the unique

identifiers found in the WHOIS record and find all the domain names related to it. Finally, a list of suspects can be created by using the data.

- **Hosting details:** Another angle that investigators can examine is the domain's hosting history. What can be gleaned from this includes transfers of ownership, if any, via changes in IP addresses, registration details, and nameservers.

- **Mail servers:** When a mail server has a connection to a suspected IP address or domain, the chances are that it may also host other malicious domains. Mapping all these data points can give investigators an idea of how the cybercrime group or individual behaves.

Domain name registration, nameserver, and Autonomous System Number (ASN) information comprise yet other data points that can help investigators pinpoint who the attackers are or at the very least, create criminal profiles.

## Gathering Evidence for Legal Proceedings

When investigators have a substantial list of possible perpetrators or identified the actual attackers, the next step is to collect enough evidence to build a case. Of course, pieces of evidence would have already floated while investigators are profiling the suspects and mapping out their behaviors. But once a final list is obtained or the attacker is identified, solid pieces of evidence such as screenshots of malicious websites are required.

Investigators can get screenshots using Website Screenshot API, which allows them to get full-page and responsive images of any website. The API can get a series of screenshots over time, and when matched with the domain's date of creation, these can show how long the attack has been going on, which strengthens the case even further.

Cyber-resilience is not only about bouncing back after an attack but as well making sure that the attack won't happen again. One way to ensure that the cybercriminal is prevented from attacking again is to do everything possible to catch them.

This can be a daunting and seemingly impossible job, but remember that online outlaws are also human beings and are therefore prone to errors. They will eventually leave digital fingerprints in the form of IP and email addresses, ASNs, and other data points.

With the right tools such as Domain Research Suite and Reverse WHOIS Search, among others, cybercriminals can be caught.