Toolbox Cloud Browser
Counterfeiting Center
http://countfe766hqe4qd.onion/
Toolbox
United States
Tor
countfe766hqe4qd.onion
COUNTERFEITING CENTER
NEW LIFE
OFFSHORE ACCOUNTS
PASSPORT
AUTHENTIC
Documents - Degrees - Hacking - Travels - Cards/Money Transfer - Offshore - Banknotes - Escrow - Buy Bitcoins
Counterfeiting Center. The orginal one
countfe766hqe4qd.onion

TOR. Use caution with content viewed/saved and follow all local/Federal laws.

Original Passports

full registered in gov database

Canada/USA/Mexico Passports	0.019 ฿
UK/European Passports	0.0152 ฿
New Zealand/Australian Passports	0.0209 ฿

Permanent Residency Visa

full registered in gov database

Canada/USA/Mexico Visa + SSN/CPN	0.019 ฿

User Agent: TOR Browser

Language: en-US,en

Timezone: America/New_York

Egress Location: Tor US East

silo

BY AUTHENTIC8

The online investigators' definitive guide to the dark web

Everything you need to know about the dark web and how to conduct secure, anonymous and efficient research

Table of Contents

The dark web may seem like a mysterious and dangerous entity to some. For investigators it can be the key to their research.

There are inherent risks involved with accessing the dark web, but with the right knowledge and capabilities — and the right policies and procedures in place — those risks can be mitigated and its usefulness to investigations unlocked.

Through this guide, we will explain the significance of the dark web to investigators, what the different darknets are and what can be found there, plus what to consider before diving in. We'll also cover how to create a dark web access policy, what not to do while on the dark web to run afoul of policy or the law. Lastly, we'll look at some of the essential tools you'll need to complete your investigation.

What is the dark web?

The dark web is an area of the internet only available via software clients. It is most notoriously known for the illegal activity it sometimes facilitates. However, there are practical uses for its existence as well, and industry professionals can benefit from becoming familiar with the crucial information that may be lurking there.

Perhaps best known for its association with criminal activity, platforms such as The Silk Road have become infamous for their use of the dark web in the illegal drug trade. But there are less nefarious reasons to access the encrypted darknets. In many countries it allows demonstrators to subvert authoritarian regimes and provides a free and open internet model that can evade censorship and provide privacy.

The sites that make up the dark web are similar in content and style to the surface web, or the internet most people are familiar with, but the traffic is routed and shared differently, making it more difficult to shut down or find the original sources of content.

For investigators, it can hold crucial information that would be otherwise inaccessible. To acquire these datasets, it is important to understand each area of the web, the different clients available to use them and what precautions should be taken before diving in.

WHAT’S THE DIFFERENCE? SURFACE, DEEP AND DARK WEB

Surface web: the internet most of us use daily (a.k.a open web, clear web). It’s the traditional format of the web, composed of open pages easily accessed by search engines on any browser.

Deep web: sites that require login or subscription services, such as court record databases. It has some barriers to accessibility while being adjacent to the surface web and is typically accessed via the same browsers.

Dark web: the area of the internet that can only be accessed by using a specific software. There are different versions available, from the most well-known (e.g., Tor/The Onion Router) to the lesser used (e.g., Freenet, I2P, ZeroNet).

Dark web networks: their risks and rewards

To access the dark web, a special software or client is needed. Each version of the dark web provides its own dataset, encryption services and risks from attempting to access it.

Tor, The Onion Router

The most commonly used darknet service is Tor (pronounced /tôr/). It stands for The Onion Router, developed by the U.S. Naval Research Laboratory in 2002. It was created to provide layers of encryption (hence the reference to onions) in order to anonymize communication between intelligence professionals.

HOW IT WORKS

Tor routes traffic through layers of nodes to create better anonymity to its users and sites. It is the largest dark web service, and everything from file shares to organizing political dissidents to dark marketplaces may be found there. Because it is the largest, it may be the most likely place to begin your dark web research.

THE DANGERS

Even with all its layers of encryption, there are still security threats and tracking mechanisms in play. There are still ways of applying analytical methods on unique identifiers to track individuals, making it essential to take security into account when accessing the service.

WHAT YOU'LL FIND

Tor is the most widely used darknet, for everything from selling contraband, spreading malicious content or receiving information from dissidents in authoritarian countries.

ZeroNet

A lesser-known darknet. ZeroNet is a peer-to-peer-based web hosting model that doesn't use IP addresses or domains for websites. Sites are not hosted via a typical service and can only be accessed by public key. It makes sites free to create and share and almost impossible to shut down.

HOW IT WORKS

To access ZeroNet, you can use a regular browser with the application running in the background. Information from it can also be downloaded and made available offline. The content is made available via BitTorrent, which shares bits of information across many peers, each one hosting a piece of the information needed. By distributing the information through many hosts, it makes it nearly impossible to track down or scrub all of the pieces of content from the web.

THE DANGERS

Investigators should keep in mind that ZeroNet is not anonymous by default when trying to access these private and public encryption keys.to take security into account when accessing the service.

WHAT YOU'LL FIND

The ability to keep content and access it offline once it is downloaded is another aspect that can be helpful for both good and bad actors. Terrorist organizations have begun to utilize this aspect, including ISIL (Islamic State of Iraq and the Levant).

I2P, Invisible Internet Project

Another darknet is I2P, or the "Invisible Internet Project," released in 2003. Unlike the previous two sources for websites and file sharing, I2P focuses mostly heavily on encrypting communication between users. Unlike Tor, it encrypts via a peer-to-peer model instead of a single thread.

HOW IT WORKS

Access to I2P uses a browser and an application in the background. It provides untraceable communication by establishing one-way tunnels through peers. Each client becomes a node in the tunnel and tunnels then expire after 10 minutes. The system is referred to as "garlic routing." The one-way messages are encrypted for recipients, as well as their delivery instructions.

THE DANGERS

End-to-end encryption cannot be guaranteed and can inadvertently lead to sharing resources with hackers or terrorist groups.

WHAT YOU'LL FIND

The communication on I2P is popular among criminals and those trying to circumvent censorship laws alike. Cybercriminals sometimes use the service to communicate about breached data, vulnerabilities or to sell malware; whereas dissidents may use it to speak out and receive unfiltered news.

Freenet

Freenet is another peer-to-peer network for sharing decentralized data created in 2000. It is used in two forms – the "opennet" allows connection to any user, while the "darknet" connects only to friends. The ability to access only known contacts, provides a higher degree of trust than other softwares.

HOW IT WORKS

Access is created through a backend web application and requires a key to access. While it was originally used by dissidents to circumvent censorship laws, it is now popularly used by cybercriminals to offload stolen and malicious content.

THE DANGERS

Like I2P, Freenet is an application that runs in the background while utilizing existing browsers. This source is popular for "off-network" data storage. It can be useful for sharing large files privately, which can be for less notorious uses but is also popular amongst criminals.

WHAT YOU'LL FIND

Cybercriminals specifically employ Freenet to deliver illegal and malicious content to verified customers. However, the service was originally used by dissidents to avoid censorship laws.

Benefits of accessing the dark web for online investigations

Each of these darknet services can benefit investigators. They can help to evaluate leads, corroborate or disprove information and track data leaks. They can also provide context of how criminal marketplaces are operating and what tactics are being used to commit hacks and fraud.

When conducting an investigation, professionals have a vested interest in finding all information and context available. Where we look can be crucial to the success of an investigation, including in online sources. For the best outcome it's important to become familiar with each layer of the web and how to search within them.

Many hackers discuss trade secrets in dark web forums. This information can help mitigate cyberthreats before they are committed or be used to recover leaked data from a breach. They may also post leaked passwords and accounts or sales of hacked devices. Financial crimes are often the subject of posts too. Stolen online bank account access or credit cards may be traced on the dark web.

When tips come in, following them in all places they lead may necessitate dark web access and help gain information on how bad actors operate. Rather than leave those crucial bread crumbs unfollowed, investigators should learn how to safely access the dark web and what a powerful tool it can become.

DON'T BE AFRAID OF THE DARK

The dark web is most notorious for illicit activity and nefarious figures (although this isn't its only purpose). Figuratively waltzing into a hotbed of criminal activity is reasonably intimidating and there are legitimate risks associated that we'll outline below.

However when conducting an investigation, one of the most efficient tools at your disposal is to go where the crime, fraud or illicit activity is taking place. If you need to learn more about a specific suspect or a leak, taking your investigation to where the bad actors commonly reside seems simply makes sense. With the right understanding of risks and precautions, you can enter the dark web to benefit your mission without compromising your security.

Combining dark web and OSINT

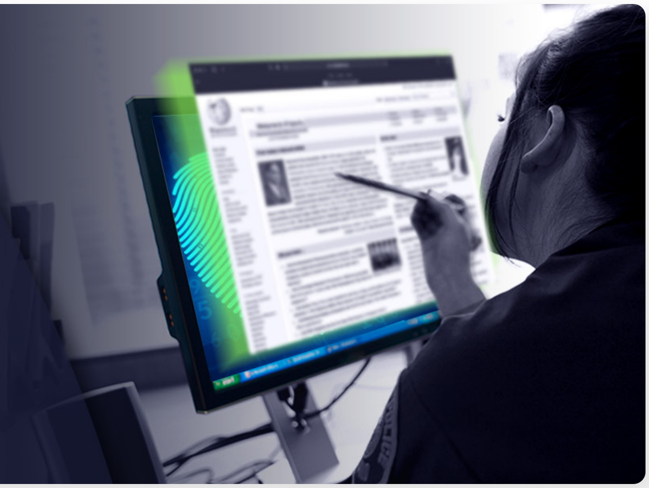
Any good investigator may already find themselves among a sea of information and may even be conducting open source intelligence gathering (otherwise known as OSINT, intelligence gathered from sources that are free and publicly available). It's important to remember that the dark web is part of OSINT — there is plenty of information to be found on sites open to anyone looking; however, the webmaster may be looking back.

Investigators need to protect themselves, their organization and their research and control the details they disclose to sites in the course of their investigation. Without proper management of their digital fingerprint, the unique identifying factors being left on the web, adversaries and investigative targets could use disclosed details to uncover their identity and intent, spoil the investigation or seek retribution.

Additionally, accessing the dark web has its own considerations in regards to internal policies as well as legality. To not run afoul of compliance teams, regulators or law enforcement, proper policy and audit capabilities need to be in place, including the ability to track what has been gathered and when.

WHAT'S IN YOUR DIGITAL FINGERPRINT?

Your digital fingerprint or browser fingerprint includes everything from which sites you click on (and which ones you skip) to the type of connection you use (IP address and provider), your hardware (device type, OS, video and audio cards), configurations (keyboard and language settings, time zones, etc.), installed software and plugins, and even seemingly random things like battery status. All of this information helps browsers track you across sessions.



silo
BY AUTHENTIC8

3 things to consider before you start your dark web investigation

Despite the benefits, many may have reasonable doubts and concerns about accessing the dark web. While accessing it is not illegal per se, it is important to take steps to mitigate any risks or potential legal threats, especially when entering areas of the dark web where illegal activity is being conducted. To avoid unnecessary risks, consider these three questions before beginning an investigation.

1 Is the dark web necessary for your investigation?

The first way to determine if accessing the dark web is for you is simple — is it the only place that offers the information you need? The dark web itself only accounts for a small amount of all internet data, just 0.01% according to Britannica. That means, when determining where you need to look, statistics are on the side of what you already have available. Most of the data you seek is likely on the surface web most people are familiar with or the deep web.

The deep web, residing just below the surface, requires login credentials to access. Many investigators use tools from the deep web, such as academic journals, crime databases or members-only social media sites and blog forums to aid in their research.

With so much of the internet freely available, you may not even need to take on the risks of trying to access a darknet. The simple answer is always the best answer — if you don't need to access it, you shouldn't. However, if the leads you chase are constantly dipping below the surface, there are ways to protect yourself and your company while following your investigation in every direction it may take you.

2 Do you fully understand the risks of the dark web?

If you have already determined that what you are looking for can only be located on the dark web, you need to understand the risks before diving in. Many dark web services — including the largest, Tor — have risks involved just with signing on. Those may include both risks to you personally and risks to your employer. Before you begin, make sure you fully understand what's at stake.

The dark web, like anywhere on the internet, comes with cyber risks. Just clicking on a link or visiting a site could introduce malicious content to your machine and network. And due to the dark web's more unscrupulous users looking to ward off any unwanted attention, it may be particularly rife with cyberthreats. Simply logging in with your main work computer or with your personal laptop without any additional precautions could introduce risk to your environment or reveal company secrets or personal information.

The next thing to consider is your digital fingerprint. Your IP address, your browser history and cookies are all giving away information about you that you may not want to be found out. Even the language your device is set to or what browser you choose may give away important context that could tip off investigative targets as to who you are and why you're on their site. This could lead not only to retaliation (cyber or physical) but may disrupt the investigation due to disinformation or a target going into hiding.

Beyond malware and hacking risks, there are still other issues to consider. For instance, if accessing blogs or marketplaces known for criminal activity, you yourself might be assumed to be a criminal by law enforcement officials. You also need to be sure dark web investigations are covered in your organization's IT policies and any necessary monitoring and auditing are in place.

Before accessing the darknet, make sure both you and your company are familiar with all risks involved and have created a detailed game plan for how to mitigate them.

3 Will you be able to conduct dark web investigations safely?

With all the risks in mind that go along with logging on to the dark web, it's important to ask if you will be able to protect yourself and your employer properly before you begin. Do you have a process in mind? Has legal counsel been consulted? And do you have a resource for concealing your identity and protecting yourself from malware?

To mitigate risks, there are a few things to consider — security, anonymity, legality and compliance.

Security through web isolation

Ensuring your browsing is 100-percent isolated from your corporate device and network is the only way to be certain that cyber risks are completely eliminated. Using a cloud-based browser allows for safe browsing of the internet while providing users with a familiar experience and much-needed protection against cyberthreats. By isolating a user's session on cloud infrastructure, clicking on a malicious link from a web search or visiting a malicious website doesn't put their organization at risk — the code from that website is never executed on the computer being used.

Instead, the user is merely seeing and interacting with a benign video display of the web code rendered in the cloud.

Anonymity through managed attribution

Hopefully this paper has made clear that the dark web does not give users complete anonymity. There are still plenty of ways darknets track users and relay information to webmasters. To conceal your identity and the purpose of your dark web investigation, researchers need to manipulate the details of their digital fingerprint.

There are ways to achieve managed attribution without needing to create a fake persona (which most social media companies are apt at finding these days) or using a burner device. Managed attribution allows you to control what can be learned about you as you conduct your dark web investigation, providing anonymity without making you appear suspicious to algorithms or your subject.

Legal and compliance considerations

Work with your company's legal counsel to create a protocol for when and how to access the dark web. Create a detailed process to work as a guide for investigators. Be sure to document each step of your investigation and keep notes about how your activity is in line with the company policy. Purpose-built online investigation solutions like Silo for Research come with policy and audit features — as well as the needed security, managed attribution and workflow capabilities — baked in.

What may be seemingly obvious is still worth stating — even when communicating in forums where criminal activity may be taking place, be sure to stay on the right side of the law. Again, documentation can go a long way in protecting you should any questions of legality arise.

Luckily the same programs that protect your digital security can also help assist in this area.

Only after you've determined whether you need to access the dark web, you understand the risks and can do so safely, should you begin to venture into the dark.

Best practices for creating a dark web access policy

A formal, dark web access policy not only sets expectations and guidance on safe practices for end users, but also helps inform and alleviate concerns from other stakeholders in an organization who may only be familiar with the dangers of the darknet — and not its value to strategic investigations.

Of course, policy must be implemented to be effective. In this case, that means not only having the right technical tools for the job, but also the training, techniques and procedures to execute safely and effectively.

Last year, the Department of Justice's Cybersecurity Unit issued guidance to the private sector on gathering cyberthreat intelligence in dark marketplaces. You can read the complete memo here. The DOJ's recommendations are helpful for organizations to consider when crafting a dark web access policy and forming best practices laid out below.

(The memo and following discussion does not constitute legal advice. Authentic8 is prohibited from offering you legal advice. Please consult your attorney or your organization's attorney for legal advice before undertaking the activities considered here.)

CREATE "RULES OF ENGAGEMENT"

"If your organization conducts activities described in this document, or is planning to do so, it should prepare 'rules of engagement' or a 'compliance program' with protocols that outline acceptable conduct for its personnel and contractors who interact with criminals and criminal organizations. Following deliberately crafted protocols that weigh legal, security and operational considerations beforehand will discourage rash decisions that could put an organization, its employees and its data in jeopardy. Having documented rules may also prove useful if the organization ever faces criminal, civil or regulatory action."

ENGAGE WITH LAW ENFORCEMENT

"It may also be beneficial to inform law enforcement before engaging in these intelligence-gathering activities by building an ongoing relationship with the local FBI field office or Cyber Task Force and the local U.S. Secret Service field office or Electronic Crimes Task Force. Early engagement with law enforcement may also help ensure that a practitioner's activities do not unintentionally interfere with an ongoing or anticipated investigation by law enforcement."

GET APPROVAL FROM LEGAL COUNSEL

"An organization should also establish policies and protocols that have been vetted with its legal counsel to guide its employees' and contractors' activities on forums (and anywhere else). Having vetted 'rules of engagement' or a 'compliance program; can help prevent personnel from accidentally or unintentionally putting their organization and its employees in legal jeopardy or risk compromising its security."

DOCUMENT PLANS AND ACTIVITY

"[Practitioners should] document their operational plans for conducting cyber threat intelligence gathering and keep records of their online activities and how information was gathered and used. In the event of a criminal investigation, such records may help establish that their conduct was legitimate cybersecurity activity and help law enforcement determine that a practitioner's actions were executed in furtherance of the company's legitimate cybersecurity operations, as opposed to the actions of a rogue employee engaged in illegal conduct."

—DOJ Cybersecurity Unit

Keeping these recommendations in mind when developing a dark web access policy will help mitigate risk and protect your organization.

4 THINGS YOU SHOULDN'T DO ON THE DARK WEB

Avoid a world of trouble by following these four simple recommendations of what not to do on the dark web during online investigations.

1. **Don't access forums in an unauthorized manner**
   If you come across a forum on the dark web that requires a credential for access, do not attempt to evade the authorization requirements.

2. **Don't assume someone else's identity**
   If you need a persona to access or interact on the dark web, don't use someone else's identity (name, photo, phone number, email, etc.) to do so without their consent. It can not only create legal trouble for you, but also could make that person a target of the criminal actors you interact with. The best approach for the dark web is to create an entirely fake persona that cannot be connected to you or your organization.

3. **Don't do research without a plan**
   Having a set of written guidelines will help keep your research efforts focused and within the bounds of your organization's risk appetite. Documented plans, policies and procedures are also helpful in the event you or your organization comes under investigation from law enforcement.

4. **Don't put your corporate network at risk**
   This one is up there with the "goes without saying" category of what not to on the dark web. But you can never be too careful, especially when it comes to activities that pose both technical and operational risks like dark web investigations. Take proper precautions.

silo
BY AUTHENTIC8

Essential tools for improving dark web research

For investigators scouring the web for clues, time-saving tools and tips can make the difference that leads to a successful inquiry. There are several tools that can unlock the data lurking in the background and help you find the breakthrough you're looking for in your search. These tips can help with easier and safer ways to search the internet — including the dark web — and discover who may be behind nefarious content.

With these simple tools, investigators can find site owners of surface sites, see bitcoin transactions and discover details behind photos on the web.

Cryptocurrency and its role in money laundering

Cryptocurrentcy, once a fringe anti-big banking trend, has taken a sharp rise in popularity over the last decade. According to Chappuis Halder, it has now grown to more than 69 million users worldwide.

The decentralized privacy offered by Bitcoin and it's crypto competitors have also become popular as money laundering tools. The anonymity of cryptocurrency provides cover for traders and a convenient way to purchase illicit substances. When tracking cybercriminals or potential hackers, the flow of currency behind major leaks or bad actors could prove insightful.

Bitcoin Who's Who

Bitcoin Who's Who allows investigators to search for identifiers from bitcoin blockchains. If a bitcoin address holds any identifying information, investigators can find it here. It also offers reports on scam alerts connected to the account. You can check the wallet balance, owner information and set up transaction alerts to notify you when exchanges with the account are made.

Other fields of interest in a Bitcoin Who's Who report include the last known IP address used in a transaction and any website where the address has appeared. This can help identify if the address is being used for sinister purposes.

Blockchain Explorer

Blockchain Explorer lets researchers search blockchain details of major cryptocurrencies including Bitcoin and Ethereum. Explorer captures historical prices, the most recently mined blocks, the mempool size of unconfirmed transactions and data for the latest transactions.

Researchers can search by block number, address, block hash, transaction hash or public key to find out more information on cryptocurrency transactions.

Using exif data to gather intel

Behind every image on the internet — on the surface as well as dark web — is valuable data which holds information about where the photo was taken, when, the file size and often what specific camera was used. These details are captured in exif — or "exchangeable image file format" — data. This hidden information can provide helpful leads for investigators.

By using tools like FotoForensics, researchers can analyze the exif data on photos to help inform investigations.

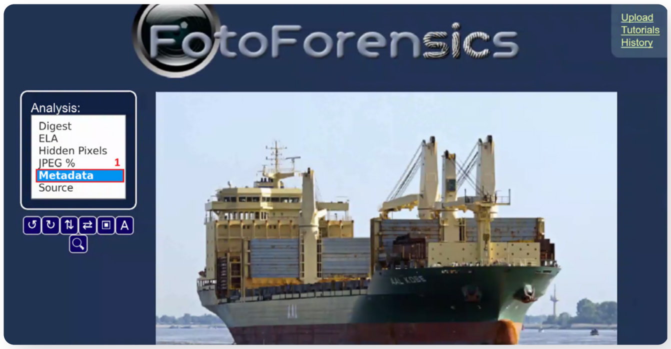
FotoForensics

FotoForensics provides detailed reports on the exif data embedded in photos. There are two ways to glean a report: Users can upload the saved image directly or paste the image URL.

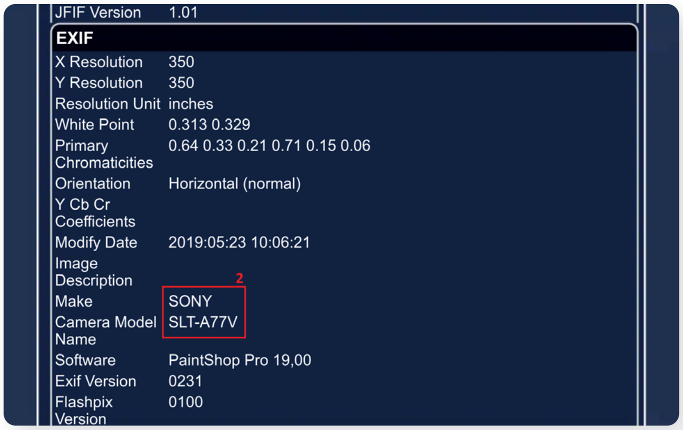
The report provided may include the geolocation in the form of coordinates. (These coordinates plugged into Google maps can provide the exact pinpoint on a map.) It also includes the time stamp and camera make and model. This analysis can provide a wealth of data about otherwise anonymous pages.

See a real-world scenario of using exif data provided by FotoForensics to decipher intelligence regarding a cargo ship image

When conducting an investigation, analysis tools and OSINT techniques can help greatly improve the efficiency and effectiveness of research. By researching site owners, investigators may learn about patterns of activity; cryptocurrency analysis can help understand the context for how and when money is being exchanged; and exif data can help provide context and intel behind anonymous images.

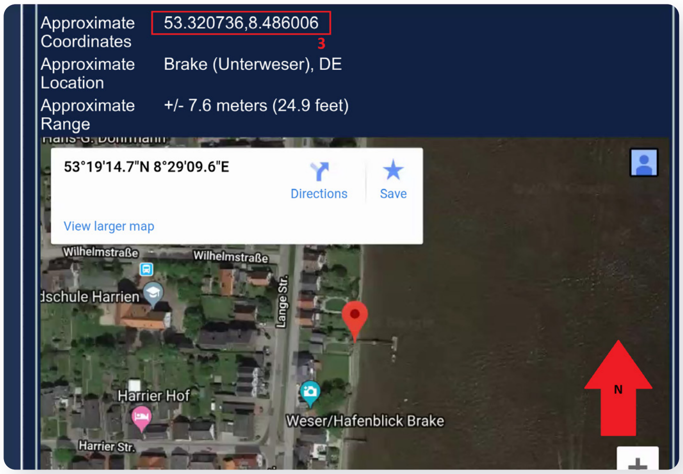


FotoForensics post image upload with metadata analysis selected



JFIF Version	1.01
EXIF	
X Resolution	350
Y Resolution	350
Resolution Unit	inches
White Point	0.313 0.329
Primary Chromaticities	0.64 0.33 0.21 0.71 0.15 0.06
Orientation	Horizontal (normal)
Y Cb Cr Coefficients	
Modify Date	2019:05:23 10:06:21
Image Description	
Make	SONY
Camera Model Name	SLT-A77V
Software	PaintShop Pro 19,00
Exif Version	0231
Flashpix Version	0100

FotoForensics exif data results including camera model



Approximate Coordinates	53.320736,8.486006
Approximate Location	Brake (Unterweser), DE
Approximate Range	+/- 7.6 meters (24.9 feet)

FotoForensics exif data results including geographic coordinates.

Safe use of the dark web

Beneath the intimidating layers and nefarious activity, the dark web can hold essential clues for investigators, making it a key place for gathering information to a successful inquiry. Whether preventing financial fraud, investigating a law enforcement matter or researching an article, the dark web holds bread crumbs longing to be followed by professional investigators.

But gathering safely is key. When diving deep, investigators must use common-sense practices, protect their anonymity and always stay on the right side of the law. Following our steps to create a policy and avoid giving away identifying information is the first step for discovering what lurks in the dark.

About Silo for Research

With Silo for Research investigators can safely explore and gather clues while protecting themselves and their companies.

Silo for Research works directly with existing IT and security programs to create access for investigators in a way that is reflective of existing company policies. It tracks activity on the dark web so investigators need not worry about audits or potential legal threats. Most importantly, it protects the identity and data of the user.

To find out more about how Silo for Research could aid your investigation, visit our site.

silo
BY AUTHENTIC8

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com