WORKSHOP ON ONLINE IPR INFRINGEMENT, DETECTION AND INVESTIGATION

KENNETH WRIGHT | BANGKOK | 10th SEPTEMBER 2019

www.ipkey.eu
BEST PRACTICES ON EVIDENCE COLLECTION, RETENTION AND PRESENTATION IN ONLINE IPR INFRINGEMENT CASES

KENNETH WRIGHT | BANGKOK | 10th SEPTEMBER 2019
1. EVIDENCE.

2. ELECTRONIC EVIDENCE.

3. INTERNET EVIDENCE.

4. CYBERCRIME CONVENTION.

5. CONCLUSION.
EVIDENCE

• EVIDENCE IS ANY PROOF.

• PROVIDED BY THE PARTIES IN LEGAL PROCEEDINGS.

• IN ORDER TO DEMONSTRATE TO THE COMPETENT AUTHORITY CERTAIN FACTS.

• ESSENTIAL TO THE CASE.
EVIDENCE

INTELLECTUAL PROPERTY EVIDENCE.

• PROVES THE INFRINGEMENT HAS TAKEN PLACE.

• PROVES WHO THE INFRINGER IS.

• PROVES THE DAMAGE SUFFERED BY THE IP OWNER.
EVIDENCE

• SURVEILLANCE (MONITOR).

• COVERT INVESTIGATIONS (TEST PURCHASE).

• RAIDS.

• SEARCH.

• SEIZURES.
1. EVIDENCE.

2. ELECTRONIC EVIDENCE.

3. INTERNET EVIDENCE.

4. CYBERCRIME CONVENTION.

5. CONCLUSION.
ELECTRONIC EVIDENCE

• ANY INFORMATION.

• GENERATED, STORED OR TRANSMITTED IN DIGITAL FORM.

• THAT MAY BE NEEDED TO PROVE OR DISPROVE A FACT.

• DISPUTED IN LEGAL PROCEEDINGS.
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE
ELECTRONIC EVIDENCE

Intermediaries at the user level dealing with receiving and presenting data to the internet users

- E-commerce platforms
- Social media platforms
- Search providers
- Transaction providers

Intermediaries at the technical level dealing with the routing and transport of data

- ISPs
- Domain name registries
- DNS managers
- VPN services
- Hosting providers
ELECTRONIC EVIDENCE

- Content data
  - E-mails
  - Chatlogs, e.g. P2P, Application and In-game Chats
  - Webform Data
- Communication data
  - Name, Address and Phone
  - Bank, Public Utility, ID and Passport Info
  - Domain Name, IP Address, IMEI, PUK and MAC Codes
  - Origin Info: Time, Date, Location and Port
  - Connection Logs Data

- Media
  - Photos and Images
  - Video and CCTV
  - Texts, e.g. Notes and Documents
  - Calendar Info
  - Meta-data
- Financial
  - Credit Card Info
  - Digital Payment Wallets
  - Virtual Currency Wallets
  - Transaction History
- Other Content
  - General Backup
  - Website Dump
  - Mailbox Dump
- Subscriber Info
- Traffic Data
- Connection Data
- Electronic Devices
ELECTRONIC EVIDENCE

PRINCIPALS OF ELECTRONIC EVIDENCE:

• DATA INTEGRITY
  NO ACTION TAKEN SHOULD CHANGE ANY DATA.

• AUDIT TRAIL
  RECORD KEPT OF ACTIONS TO FACILITATE REPETITION.

• SPECIALIST SUPPORT
  SUSPECT YOU WILL ENCOUNTER ELECTRONIC EVIDENCE.

• APPROPRIATE TRAINING
  FIRST RESPONDER, IN ABSENCE OF SPECIALIST.

• LEGALITY
  LAW AND PROCEDURES MUST BE OBSERVED TO ENSURE ADMISSABILITY.
1. EVIDENCE.

2. ELECTRONIC EVIDENCE.

3. INTERNET EVIDENCE.

4. CYBERCRIME CONVENTION.

5. CONCLUSION.
Novotel Bangkok Ploenchit Sukhumvit, a conveniently located Bangkok Hotel, nearby

Novotel Bangkok Ploenchit Sukhumvit
566 Ploenchit Road, Lumpini, Patumwan,
INTERNET EVIDENCE

WEBSITE.

• REGISTRAR.

• REGISTRANT (FAKE?).

• REGISTRATION DATE.

• DOMAIN NAME / IP ADDRESS.
INTERNET EVIDENCE

WHOIS Search, Domain Name, Website, and IP Tools

https://www.novotelbangkokploe

Your IP address is 45.112.143.2
Hello, Get a Rs.100 Amazon Pay Gift card with Vodafone Prepaid

To: esha.pathak.2@yahoo.co.uk, Esha Pathak

Open In Another Tab

To Whom It May Concern,

I am writing to inform you about a special offer from Vodafone Prepaid. For a limited time, you can get a Rs.100 Amazon Pay Gift card with Vodafone Prepaid services. This offer is available for a limited period, so I urge you to take advantage of this opportunity.

Please note that this offer is subject to certain terms and conditions. You can find more details about the offer on the Vodafone Prepaid website.

Thank you for your time and consideration.

Best regards,

Esha Pathak
INTERNET EVIDENCE

How To Perform A Reverse Email Lookup

Step 1: Locate the email address you want to lookup.
Step 2: Copy and paste the email address in the search box below.
Step 3: Click the "Search" button to display the results.

Enter email address

*Please note the search is free, but opting for a report will result in a charge to your preferred method. Pricing for the highly accurate reports is shown at checkout, but contain thorough information and require payment to proceed.

How To Perform An Email Header Trace

Step 1: Locate the email header (see example further down).
Step 2: Copy the email header and paste in the search box below.
Step 3: Click the "Trace Email Sender" button for the results.

eDgS8Bomm7100xRoQDxP1VD1aexfTw40jnf1S4ymid25EyHu0JAJV8g z177EwAF+ts5bM19yx10j
PVa578BE17Jli9l9W7Q1jPQSzb3LiJlvxhUTakMFEVWxjJ1Sidw8tgc nbzh2KtHK4FZPuZI
WWUOlil8B84Ppyw9YYeLqoRyGxKhHcdcvseDCnNlIDZ2FP2r2DSF8y M1ZI63uO3W6/Us9rgTLPL
				tunQ8EtekRfFe24Tq1/y8GSvXwabsbITKJIg==

Verify  Clear
<table>
<thead>
<tr>
<th><strong>Email Sender</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>103.107.120.134</td>
</tr>
<tr>
<td><strong>IP Address Country</strong></td>
<td>India</td>
</tr>
<tr>
<td><strong>IP Address State</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IP Address City</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IP Address Postcode</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IP Address Latitude</strong></td>
<td>20.0000</td>
</tr>
<tr>
<td><strong>IP Address Longitude</strong></td>
<td>77.0000</td>
</tr>
<tr>
<td><strong>ISP of this IP</strong></td>
<td>Instant Technosoft</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Instant Technosoft</td>
</tr>
<tr>
<td><strong>Timezone</strong></td>
<td>Asia/Calcutta</td>
</tr>
<tr>
<td><strong>Local Time of this IP country</strong></td>
<td>2019-09-10 00:02:05+05:30</td>
</tr>
</tbody>
</table>
INTERNET EVIDENCE

Get more done with Gmail

Now more secure, smarter and easier to use — helping you save time and do more with your inbox.

Get Gmail
INTERNET EVIDENCE

EMAIL ADDRESS.

• GOOGLE LEGAL INVESTIGATIONS SUPPORT (LIS-GLOBAL@GOOGLE.COM).

• IP ADDRESS OF PERSON CREATED THE ACCOUNT.

• DATE ACCOUNT WAS CREATED.

• IDENTITY OF PERSON WHO CREATED ACCOUNT (FALSE?).

• PHONE NUMBER, OTHER EMAIL, LAST LOGIN, PAYMENT METHODS ETC.

• PRESERVATION REQUEST.
Internet Evidence

Facebook

Law Enforcement Online Requests

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.
If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

- [ ] I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Request Access
INTERNET EVIDENCE

SOCIAL MEDIA.

• ADMINISTRATOR OF SITE.
• DATE SITE CREATED.
• LINKS TO PERSONAL PAGE.
• PHOTOGRAPHS OF SITE ADMINISTRATOR.
• PRESERVATION REQUEST.
INTERNET EVIDENCE

TIPS:

• USE BROWSER TO SAVE A WEB PAGE - INCLUDING HTML SOURCE CODE.

• VIDEO CAMERA.

• DIGITAL SCREEN CAPTURE SOFTWARE - CAMSTUDIO OPEN SOURCE.

• CREATE AN OFFLINE COPY - HTTrack WEBSITE COPIER.
1. EVIDENCE.

2. ELECTRONIC EVIDENCE.

3. INTERNET EVIDENCE.

4. CYBERCRIME CONVENTION.

5. CONCLUSION.
CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION) (JULY 2004).

- SEEKS TO ADDRESS INTERNET AND COMPUTER CRIME.
- HARMONISING NATIONAL LAWS.
- IMPROVING INVESTIGATIVE TECHNIQUES.
- INCREASING COOPERATION BETWEEN NATIONS.
- 64 STATES (RATIFIED) (PHILIPPINES).
CYBERCRIME CONVENTION

CRIMES.

• ILLEGAL ACCESS AND INTERCEPTION.
• DATA AND SYSTEM INTERFERENCE.
• MISUSE OF DEVICES.
• COMPUTER RELATED FRAUD AND FORGERY.
• CHILD PORNOGRAPHY.
• COPYRIGHT AND NEIGHBOURING RIGHTS.
CYBERCRIME CONVENTION

PROCEDURAL TOOLS:

• EXPEDITED PRESERVATION.
• SEARCH AND SEIZURE.
• PRODUCTION ORDER.
• INTERCEPTION OF COMPUTER DATA.
INTERNATIONAL COOPERATION:

• EXTRADITION.
• MLA.
• EXPEDITED PRESERVATION.
• MLA FOR ACCESSING COMPUTER DATA.
• MLA FOR INTERCEPTION.
• 24/7 POINTS OF CONTACT.
CYBERCRIME CONVENTION

- Secure crime scene
- Document and draw plan of the scene. Take photographs of the scene, devices and screens.
- Check if machines are running:
  - Is screen on and connected?
  - Move mouse to activate screen
  - Check for indicator lights
  - Listen for activity noise
- Are machines running?
- Yes → Follow guidance in "Live Forensics flowchart"
- No → Do not turn on the computer
CYBERCRIME CONVENTION

Label connections, cables of computers and attached devices

Photograph and document the labeled computers and attached cables, connections and devices

Pull the power plugs from the back of the machines and remove all cables

Bag, tag and transport all electronic evidence in accordance with agency procedures

Follow guidance in "Acquisition of digital storage media"

Reminder:

Remember to collect all forms of potential electronic evidence such as:
USB storage media, optical discs, mobile phones, tablets, laptops, SD and similar cards, NAS

Consider other forms of forensic evidence such as: fingerprints and DNA before collection of devices.

Consider other forms of associated evidence such as: passwords, notes, paper documents, other information relevant to the investigation.

For detailed guidance see chapter 4
CONNECT FORENSIC CLONING DEVICE
OR HARDWARE WRITE-BLOCKER

INSERT WIPE HARD DISK IN THE
CLONING DEVICE OR IN THE
FORENSIC WORKSTATION

GENERATE EXACT COPY OR
FORENSIC IMAGE USING COURT
VALIDATED HARD- OR SOFTWARE
TOOLS.

WILL THE ORIGINAL REMAIN
SEIZED?

YES

NO

ONE COPY

TWO COPIES

VERIFY THE CLONES OR FORENSIC
IMAGES BY HASH CALCULATION
AND COMPARISON

SECURELY PACK THE IMAGES

SECURELY TRANSPORT THE IMAGES
TO THE FORENSICS LAB, EVIDENCE
VAULT, NOTARY’S OFFICE OR COURT
OBTAINING THE CHAIN OF CUSTODY
1. EVIDENCE.

2. ELECTRONIC EVIDENCE.

3. INTERNET EVIDENCE.

4. CYBERCRIME CONVENTION.

5. CONCLUSION.
CONCLUSION

1. EVIDENCE PROVES AN INFRINGEMENT HAS TAKEN PLACE.

2. EVIDENCE PROVES WHO THE INFRINGER IS.

3. EVIDENCE PROVES THE DAMAGE SUFFERED BY THE IP OWNER.

4. THE LAW FACILITATES THE COLLECTION OF EVIDENCE.

5. ELECTRONIC EVIDENCE IS KEY TO AN ONLINE INVESTIGATION.

6. SPECIALIST PROCEDURES NEED TO BE ADOPTED FOR ELECTRONIC EVIDENCE.
THANK YOU

@IPKey_EU