STEGANOGRAFIE VE VIRTUÁLNÍM PROSTŘEDÍ INTERNETU

STEGANOGRAPHY IN VIRTUAL ENVIRONMENT OF THE INTERNET

ADAM OMASTA
National Drug Headquarters, Criminal Police and Investigation Service, Police of The Czech Republic

Abstrakt: Od starověku až po dobu digitálního věku lidé využívali různé techniky k ochraně informací ukrýváním tak, aby zastírali jejich existenci. Dnes je steganografie využívaná i v rámci kybernetické kriminality nebo jiné kriminality páchané za pomocí informačnía komunikační technologie. Oproti steganografii stojí stegoanalýza, která má za cíl takto ukryté informace detekovat. Metody takovéto detekce jsou aplikovány na kazuistice události 11B-X-1371, která se stala doménou komplexní stegoanalýzy.

Klíčová slova: *steganografie; stegoanalýza; metadata; exif; OSINT; zpravodajství z otevřených zdrojů; SOCMINT; zpravodajství ze sociálních médií; 11B-X-1371; videoanalýza; CTF; ICT; kryprotgrafie*

ÚVOD

Steganografie a stegoanalýza nejsou příliš známé názvy v rámci analýz u kriminální policie a právě data z takovýchto analýz mohou stát za velkou policejní výzvou ve světě zločinu. U tak rozsáhlého tématu, jako jsou právě zmíněné metody, je nemožné zakomponovat hlubší poznání. Cílem tohoto článku je uvést čtenáře do počátku a vývoje steganografie a seznámit je s aktuálními trendy tohoto tématu. Autor článku se v roce 2015 zapojil do stegoanalýzy projektu „11B-X-1371“ jako člen mezinárodního komunitního týmu složeného z amatérů zabývajících se právě těmito rébusy virtuálního prostředí internetu, a proto je možné v článku uvést praktickou aplikaci stegoanalýzy krok za krokem projektu „11B-X-1371“.

POČÁTKY STEGANOGRAFIE A JEJÍ VÝVOJ

Steganografie je částí kryptografie, jejíž název se odvozuje ze spojení řeckých slov „stegos“, v překladu skrytý, a slova „grafia“, což je psaní. Zatímco kryptografie se soustředí na šifrování zpráv tak, aby bez potřebných vstupních dat nebylo možné zprávu přečíst, steganografie je způsob ukrytí zprávy, ať už šifrované či nikoliv tak, aby při prvním pohledu na nosič takové zprávy nebylo zjevné, že se o zprávu jedná. Cílem steganografie je ochrana zprávy před jejím zadržením či zničením. Celým procesem odhalování ukrytých dat se zabývá vědní obor stegoanalýza, která je velmi náročnou disciplínou. Tak jako každá vědní disciplína i steganografie prošla napříč historií svou proměnou, a to od primitivního ukrývání zpráv bez potřeby speciálních nástrojů až po pokročilou formu digitální steganografie, která vyžaduje speciální znalosti včetně informační a komunikační technologie, dále jen mezinárodní zkratka „ICT“.

Mezi nejznámější historické události ze starověku z oblasti steganografie nepopíratelně patří

ISSN 1211-8834

zpráva Histiaea, řeckého vládce města Milétu z 6. století před naším letopočtem, který v době iónského povstání využil z dnešního hlediska velmi primitivního způsobu steganografie pro zaslání zprávy svému spojenci s varováním do Milétu. Svou zprávu vyslal za pomoci jemu nejvěrnějšího otroka. Otrokovi ostřihali hlavu a zprávu mu vytetovali na kůži týlu. Poté vyčkali, až mu vlasy dorostou a následně byl sluha vyslán k příjemci zprávy do hlavního města vzbouřenců. Mezi další nejznámější osobnosti ve starověké steganografii patří i Herodotos, který držitel titulu „otec dějepisu", ale málokdo ví, že Herodotos svým sběrem informací odhalil invazi perského krále Xerxe do Řecka, který po 5 let tajně budoval armádu. Herodotos si byl vědom, že jakákoliv šifrovaná nebo podezřelá zpráva bude zadržena, proto tyto informace ukryl na několika dřevěných deskách, které byly zality ve vosku. Herodotos vosk odstranil, do desek vyškrábal zprávu a následně opět desky zalil do vosku. Takto ukrytá zpráva byla úspěšně doručena.[1]

V dobách středověku existovalo množství forem ukrývání zpráv za využití nejrůznějších tekutin a neviditelných inkoustů. Avšak jedna metoda si v historii našla místo pro svůj důvtip a originalitu. Giambattista della Porta, vědec a učitel, v 16. století mimo jiného sepsal dílo: „De Furtivis Literarum Notis", které se věnovalo kryptografii. Do historie se nezapsal jen kvůli této publikaci, ale zcela originálním ukrýváním zpráv. Během španělské inkvizice bylo několik jeho přátel uvězněno a věděl, že cokoliv, co přichází do cely, podléhá prohlídce a pokud se jedná o zakázanou věc nebo zprávu, je zabavena. Giambattista della Porta přišel se zajímavým nápadem. Uvařil vejce a na skořápku za pomocí octa napsal text zprávy. Skořápka je porézní a ocet se vtiskl do vejce tak, že byl text čitelný až po oloupání vajíčka.[2]

Metody steganografie se napříč historií stávaly stále více důmyslnější, a i když vám zpráva stála před očima, ani by vás nenapadlo, že se na ni díváte. Například Lord Robert Baden-Powell v dobách Búrské války kreslil do obrazů s motýly plány pevností s dělostřeleckým postavením nebo topografii terénu na nepřátelském území.[3] Obrazce byly tak dokonalé, že pokud jste skutečně nevěděli, co hledáte, ani by vás to nenapadlo.

V dnešní době, době informačního věku, se jedná o tzv. digitální steganografii, která se naprosto vymyká tomu, co historie v této oblasti zná. Asi nejzajímavějším příkladem ukrývání dat je ukládání prostřednictvím vrstev v rámci protokolů TCP/IP. Dle Buttera Lampsona jde o případy nevyužitého místa na disku, například u FAT 16, který je uspořádán v clusterech o velikosti 32 bitů, což znamená, že i data v objemu 1 bitu zaberou celkový cluster o 32 bitech. Data mohou být tedy uložena na disk bez viditelnosti v systému.[4] Stejně tak, jako je můžete uložit nepozorovaně na datový nosič, je možné je uložit do audio stopy a při testu spektrografem můžeme zjistit nejen grafické znázornění textu, ale i obrázků.

STEGANOGRAFIE V KRIMINALISTICE

Steganografie byla využívána napříč historií k ochraně veřejných zájmů nebo politickým machinacím, ovšem svou oblast uplatnění nalezla i na kriminální scéně. Od starověku až do 20. století byla tuláky a zločinci zejména z oblasti majetkové trestné činnosti využívána steganografie v primitivní formě tím, že byla označována veřejná místa různými piktogramy, které se v textuře nosiče značky ztratily a jen člověk, který věděl, kde se informace nachází, ji mohl odhalit. Tyto značky vznikaly za účelem klasifikace daného města z pohledu bohatství, povahy obyvatelstva či jak přísný je místní dohlížitel na veřejný pořádek. Také bylo možné zjistit tyto značky i na hraničních kamenech, kde doplňovaly stávající oficiální text nebo symbol.

V moderní době je steganografie spojována výrazněji s výzvědně zpravodajskou aktivitou, kdy se touto formou ve dvacátém století předávaly informace. Na rozdíl od dob tuláků se jedná o velmi pokročilou steganografii, jako jsou například mikrotečky na poštovní známce obsahující grafický

materiál nebo digitální formu steganografie ukrývaní dat na datových nosičích či ukrývání dat ve vrstvách internetových protokolů. Fenoménem moderní steganografie je i její rozsáhlá kriminalizace jako forma komunikace mezi teroristickými organizacemi anebo zločineckými uskupeními zejména v oblasti kybernetické kriminality či zločinci využívající ICT ke kriminálním aktivitám. V 21. století se steganografie mediálně spojuje zejména s náboženskými a politickými teroristickými skupinami. Hlavně pak s uskupením ideologie chalífátu, jako je Islámský stát, který touto formou rozsáhle komunikuje se svými přívrženci. Jeden z nejznámějších způsobů takovéto komunikace mezi přívrženci radikální skupiny ISIL byl skrze digitálně vydávaný časopis Kybernetiq v letech 2015 až 2017. Časopis Kybernetiq byl stejně jako jiné časopisy a oběžníky digitálně distribuovaný Islámským státem a byl určen přívržencům ideologie. Časopis Kybernetiq se lišil od ostatních tím, že neobsahoval jen návody k diverzním akcím v oblasti kybernetiky a jak se chránit před dekonspirací, ale i ukryté zprávy pro radikální spící buňky právě formou steganografie.

V případě ukrývání zpráv a dat se nemusí jednat vždy o zločinecká uskupení ve formě rozsáhlého organizovaného zločinu. Existují i zcela obyčejní pachatelé, kteří data s důkazní hodnotou o kriminálních aktivitách ukládají například v datovém kontejneru maskovaného nejčastěji jako soubor typu „dll“ ve zdrojovém adresáři operačního systému, nebo texty ukryté v souborech „epub“ maskující se jako běžná literatura do čtečky knih. V dnešní době to již dávno není doména špionážních her. S touto metodou ukrývání dat před policií se dnes setká téměř každý kriminalista, a to zcela určitě i několikrát za služební kariéru.

SVĚTOVÉ TRENDY A ZAJÍMAVOSTI

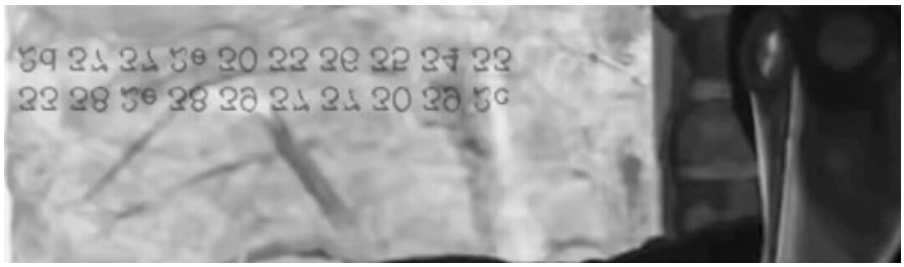
Zmiňovaná a často démonizovaná steganografie však nemusí mít jen kriminální nebo zpravodajské opodstatnění. V dnešní době existuje i velmi silná komunita zabývající se steganografií nejen jako hobby, ale i zcela profesionálně ve formě spolupráce s bezpečnostními složkami. Součástí komunit jsou i specialisté na kryptografii, kterou je steganografie součástí a která se zaměřuje na šifrování. V početné komunitě jsou i specialisté na analytické metody open source intelligence, dále jen „OSINT“, a social media intelligence, dále jen „SOCMINT“. Takovéto komunity často vyhledávají zájmové události spojované se steganografií, ať je už účelem pomoc bezpečnostním složkám nebo promoakce poukazující na humanitární či jiný sociální problém. Někdy jsou součástí takovýchto akcí i velmi složité rébusy několika úrovní, které fungují jako určitá forma výběrového řízení ke zpravodajským složkám. V tomto případě stojí za zmínku zejména událost s názvem „cicada 3301“, která byla aktivní především v letech 2012 až 2014 a kterou se nikdy nepodařilo celkově vyřešit. Zmiňovaný rébus se komplexně zaměřoval na oblast kryptografie, steganografie a rozboru dat. Cíl rébusu nikdy nebyl oficiálně zveřejněn, avšak nejzdatnější luštitelé tohoto rébusu byli téměř bezprostředně kontaktování zpravodajskými složkami USA s pracovní příležitostí.

KAZUISTIKA UDÁLOSTI 11B-X-1371

Mezi nejznámější steganografické případy patří událost, která byla spuštěna anonymně zveřejněným videem označeným jako „11B-X-1371“. V roce 2015 bylo skrze portál https://www.youtube.com sloužící ke zveřejňování video obsahu vypuštěno na internet osobou využívající pseudonym „AET-BX“ záhadné video s názvem „01101101 01110101 01100101 01110010 01110100 01100101“ o délce dvou minut, na kterém neverbálně komunikuje osoba v masce a oděvu morového lékaře. Vzhledem k tomu, že si videa příliš nikdo nevšímal, tak se osoba rozhodla video odeslat na DVD provozovateli portálu http://gadgetzz.com/, který ho zveřejnil pod názvem, jenž byl uveden DVD jako „11B-X-1371“. Video působilo strašidelně a velmi záhadně, a jak se šířilo internetem, tak si ho všim-

ISSN 1211-8834

Obr. 1 – Náhled stopy videa 11B-X-1371 počátek stopy (Zdroj: Archiv autora článku).



Obr. 2 – Kód zjištěný z problikávající zprávy (zdroj: Archiv autora článku).

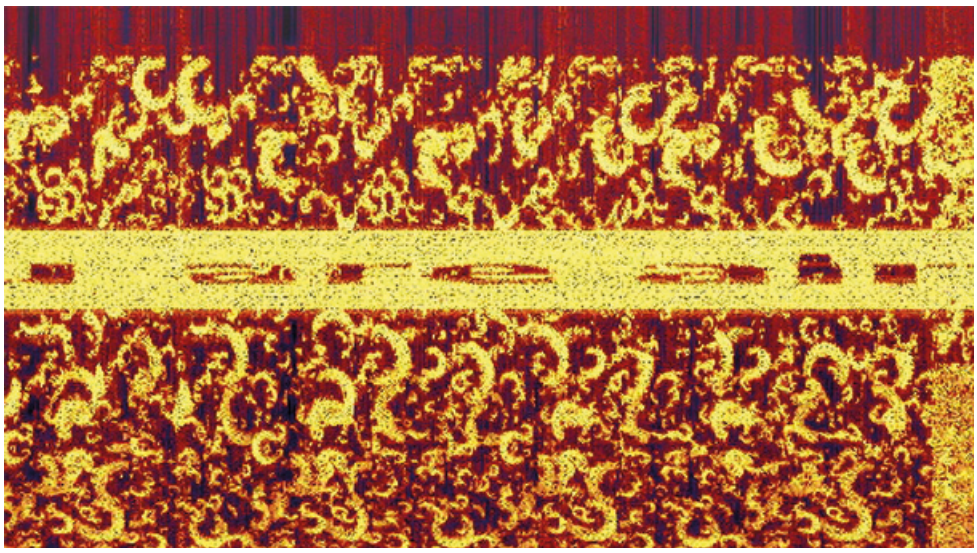
la komunita z oblasti steganografie, která jej začala analyzovat. Při prvních výsledcích skrytých zpráv toto video zaujalo rovněž zpravodajské složky z celého světa.

Video začíná stojící osobou oděnou v kostýmu a s maskou morového lékaře u okna a stěny viz obr. 1. Celé video má dvě minuty a je černobílé, v celé stopáži je mechanický zvuk. V 9. sekundě videa osoba ukazuje na pravé ruce 3 prsty, následně jeden a poté dva, mezitím v okně vedle stojící osoby problikávají písmena a čísla. V čase stopy 34. sekundy osoba zvedla pravou ruku a na dlani problikává světlo připomínající morseovku téměř 60 sekund. V čase stopy osoba na videu roztáhne ruce a v okně opět problikávají čísla a písmena a následně stopa končí.

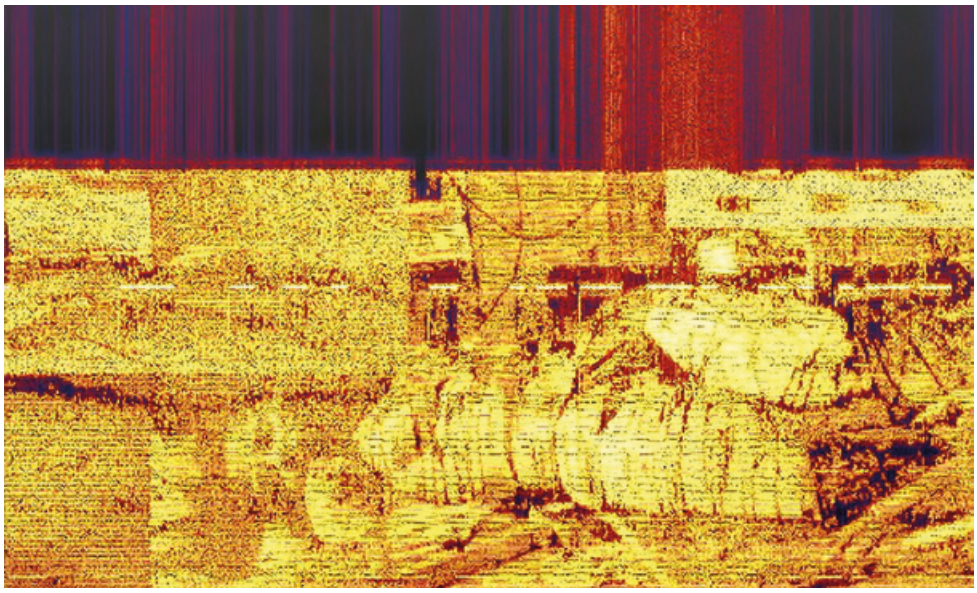
V čase stopy 28. sekundy v okně vedle osoby problikávají čísla: „33 38 2e 38 39 37 37 30 39 2c 2d 37 37 2e 30 33 36 35 34 33“, náhled obr. 2, ve skutečnosti se jedná o GPS koordináty 38.897709,-77.036543, které patří adrese: „The White House, 1600 Pennsylvania Avenue NW, Washington, DC 20500, Spojené státy americké“, na které v roce 2015 bydlel a úřadoval americký president Barack Obama.

Výše uvedeným nálezem bylo rovněž zjištěno, že každé číslo v nahrávce hraje svou roli, a proto byl zkoumán i samotný název videa, které bylo zveřejněno na portálu Youtube a to „01101101 01110101 01100101 01110010 01110100 01100101“. Následně bylo zjištěno, že v překladu z binárním kódu se jedná o španělské slovo „muerte“, přeloženo jako „smrt“.

Mezi problikávající zprávy, jako v náhledu u obr. č. 2, patří i zpráva „Red lips liketenth“, která je anagramem „Kill the president“, což je



Obr. 3 - Náhled analýzy zvuku videa spektrografem (zdroj: Archiv autora článku).



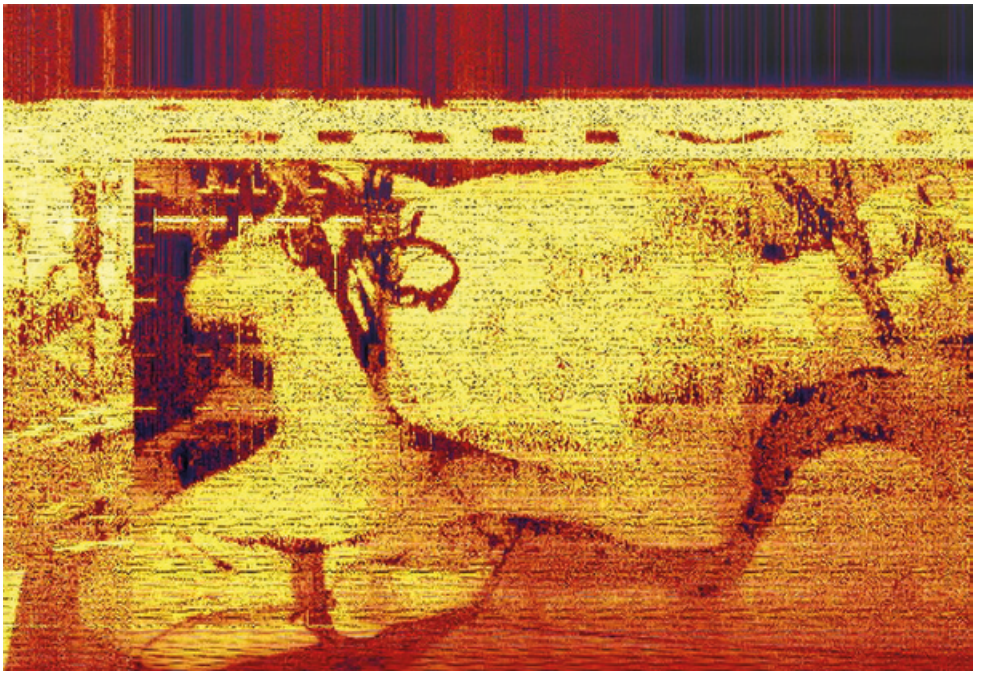
Obr. 4 - Náhled analýzy zvuku videa spektrografem (zdroj: Archiv autora článku).

z anglického jazyka přeloženo jako „Zabij prezidenta“.

Podezřelý a podivný mechanický zvuk nahrávky byl analyzován spektrografem, kdy byl touto metodou odhalen grafický materiál jiné povahy, než bylo na výše zmiňovaném videu. Náhledy nálezu spektrografu jsou uvedeny jako obr. č. 3, 4, 5.

V rámci analýzy bylo zjištěno, že v počátku stopy videa se objevuje text: „You are already death“, náhled v obr. č. 3, což je v překladu z angličtiny „Už teď jste mrtví.“. Další grafický materiál následující po této zprávě je snímek zakrvácené ženy bez údů, kde se pravděpodobně jedná o fotografii v souvislosti se spácháním násilného činu, náhled grafického materiálu na obr. č. 4. Po vyobrazení zakrvácené ženy následoval obrázek svázané ženy evidentně násilné povahy, náhled tohoto grafického materiálu viz obr. č. 5. Mezi grafickým materiálem obr. č. 4 a 5 byl umístěn nápis „We are the antivirus“, což znamená v překladu z anglického jazyka „Jsme antivirus“.

ISSN 1211-8834



Obr. 5 - Náhled analýzy zvuku videa spektrografem (zdroj: Archiv autora článku).

Obr. 6 – Náhled stopy videa 11B-X-1371 piktogram na stěně (zdroj: Archiv autora článku).

Obr. 7 – Fotografie pořízená v opuštěném sanatoriu s piktogramy z videa (Zdroj: https://www.dailydot.com (online) 7. července 2021 10:28 dostupné z https://www.dailydot.com/debug/exclusive-11b-x-1371-video-photos/)

Tyto snímky upoutaly pozornost nejen bezpečnostních složek, ale i samozvaných odborníků s konspiračními teoriemi, a to sérií násilných událostí, které se odehrály roku 1964 v americkém městě Boston, kde bylo zavražděno 13 žen uškrcením. Tyto teorie se podařilo vyvrátit týmem složeným z odborníků napříč bezpečnostními složkami USA, který právě tuto událost „11B-X-1371“ vyšetřoval. Snímek z náhledu obr. 4, byl pořízen z nahrávky filmu s názvem: „Slasher“ režiséra Farnk W. ´Montaga, který byl uveden do médií v roce 2007. Dále snímek z náhledu obr. 5 byl pořízen z nahrávky filmu s názvem: „The Bunny Game“ od režiséra Adama Rehmeiera, který byl uveden do médií v roce 2010.

Bezpečnostní složky zabývající se touto události svá šetření ukončily se závěrem, že se jedná pouze o promoakci nebo soutěž a není důvod k bezpečnostním obavám. Rovněž bylo

zjištěno místo, kde se celá událost natáčela. K tomuto odhalení dopomohl i piktogram za osobou z videa, viz obr. 6, který byl lokalizován v opuštěném sanatoriu na adrese Jana Kochanowskiego 10/16, 05-400 Otwock, Polsko viz. obr. 7.

S odstupem několika měsíců se komunitě ozval i samotný autor vystupující pod jménem Parker Wright, který doložil své autorství proprietami z výše uvedeného videa a vysvětlením, že se celou dobu jednalo o performanci z oblasti steganografie. Po této události vzniklo ještě několik videí jako 11B-3-1369 a 110A30213, ale ty už komunita nepřijala tak vřele jako událost 11B-X-1371. Po vyřešení a zjištění všech informací v rámci události „11B-X-1371" se tato komunita rozrostla tak dynamicky, že dnes jsou téměř pravidelně pořádány speciální hry CTF, což je zkratka z anglického názvu „Capture The Flag". Jedná se o specifickou formu soutěže, kde dochází k získáváním bodů na základě plnění jednotlivých úkolů, kde je cílem maximalizace získaných bodů.

ZÁVĚR

Na závěr lze konstatovat, že steganografie a stegoanalýza tak, jak na ně poukazuje článek, jsou důležitou součástí policejních činností, a to zejména v oblasti kriminalistiky. Dnešní pachatelé nemusejí být žádnými odborníky na kybernetiku a i s prostou uživatelskou úrovní ICT dokáží ukrývat data tak, aby byla neviditelná a zdánlivě se tvářila zprvu jako nezájmový objekt. Zároveň na základě těchto zjištění sledujeme pozitivní trend narůstajícího počtu kriminalistů z různých problematik, které rozšiřují své schopnosti a dovednosti právě v souvislosti s oblastí kybernetiky.

Konflikt zájmů/Conflict of Interest:
Autor prohlašuje, že v souvislosti s tímto článkem je bez konfliktu zájmů.

Corresponding author:
kpt. Bc. Adam Omasta, DiS
e-mail: adam.omasta@pcr.cz
Policejní prezidium ČR,
poštovní přihrádka 62/NPC,
170 89, Praha 7

Abstract:
From the ancient times to digital age people used various techniques to protect information by hiding them, to obscure their existence. Today steganography is using in cybercrime or other crime committed with the help of information and communication technology. In other side of steganography is standing steganoanalysis, which aims to detect hidden information. The methods of detection were applied to the case of event 11B-X-1371, which has become the domain of complex stegoanalysis.

Key words:
steganography, stegoanalysis, metadata, exif, OSINT, open source intelligence, SOCMINT, social media intelligence, 11B-X-1371, videoanalysis, CTF, ICT, cryptography

LITERATURA
1) Wayner, P. *Disappearing cryptography: information hiding: steganography & watermarking*, 2nd ed.; Morgan Kaufmann Publishers: Amsterdam, 2002. ISBN 1-55860-769-2.
2) Kipper, G. *Investigator´s guide to steganography*, 1st ed.; CRC Press Company: Florida, 2004. ISBN 0849324335.
3) Baden-Powell, G.; Baden-Powell, R. S. S. *Moje dobrodružství na výzvědách*, 1st ed.; Sfinx: Královské Vinohrady, 1920.
4) Fridrich, J. *Steganography in digital media: principles, algorithms and applications*, 1st ed.; Cambridge university press: Cambridge, 2009. ISBN 978-0521190190.

ISSN 1211-8834