Znalecký posudek

z oboru Kybernetika
odvětví Výpočetní technika

PLZEŇ

Č. j.: 4165/2018

V Plzni, dne 3. května 2018

Okresní soud Praha-východ
Na Poříčí 1044/20
112 97 Praha 1

JUDr. Haňková

Výtisk číslo: 2
Počet stran: 11

ZNALECKÝ POSUDEK

z oboru Kybernetika odvětví Výpočetní technika

Ing. Jan Janka, soudní znalec v oborech Kybernetika, odvětví Výpočetní technika a Elektronika, odvětví Elektronika, specializace Bezpečnost informačních systémů, podává tento

znalecký posudek

na základě: opatření podle § 105 odst. 1 trestního řádu v trestní věci obžalovaného: Ing. Petr Vlček, narozený 5. 7. 1974, bytem Borka 33, 251 66 Ondřejov

Č. j.: 1 T 11/2017-648 ze dne 19. 2. 2018.

1 Úvod

1.1 Věci, stopy a vzorky, které byly zkoumány

- Trestní spis

1.2 Otázky, které mají být zodpovězeny

1) Je možné, aby komunikace mezi obžalovaným a poškozenou ze dne 19. 12. 2015 ohledně sepisu anonymního dopisu, předložená obžalovaným na elektronickém nosiči dat, byla zfalšována a případně jakým konkrétním způsobem?
2) Jakým konkrétním způsobem by bylo možné zajisdt dálkový přístup k počítači poškozené ve vztahu ke komunikaci (telefonátu) poškozené s policistou Kuncem?
3) Jsou při ohledání zjištěné vzdálené přístupy do počítače ve dnech 28. 12. a 29. 12. 2015 pouze torzem původních informací o dálkovém přístupu, mohly být informace o dálkovém přístupu z počítače reálně vymazány? Lze vyloučit, že vzdálený přístup do počítače poškozené a stažení záznamu telefonátu poškozené s policistou Kuncem mohlo být učiněno kdykoli přede dnem 28. 12. a 29. 12. 2015?
4) Mohlo dojít k dálkovému přístupu k počítači poškozené a stažení výše uvedeného telefonátu jiným způsobem?
5) Jak by vzdálený přístup do počítače mohl být osobou používající počítač vnímán v intencích toho, co vypovídá poškozená?
6) Jakým způsobem by obžalovaný mohl s ohledem na pohyb mobilních přístrojů poškozené a obžalovaného (viz úřední záznam na č.l. 333 a násl. spisu) postupovat v případě, že by se mělo jednat o fingovanou textovou zprávu? Bylo by možné přihlášení na mobilní telefon poškozené v místě buňky jejího bydliště v době, kdy ho měl mít údajně obžalovaný?
7) Uveďte další skutečnosti, které považujete za podstatné z hlediska své znalecké odbornosti.

Ve znaleckém posudku je dále třeba posoudit a odpovědět na tyto otázky obžalovaného:

1) Existují jakékoliv technické podklady, ze kterých se lze důvodně domnívat, že záznamy telefonních hovorů se vůbec někdy nacházely na PC obžalovaného, užívaného poškozenou? Jsou pro tuto domněnku jakékoliv technické stopy? Uveďte které.
2) Pokud existují záznamy na PC obžalovaného, užívaného poškozenou o existenci záznamů telefonních hovorů, existují jakékoliv technické stopy směřující k domněnce, že tyto zájmové soubory na PC nahrál obžalovaný?

3) Lze zjistit, zda obžalovaný ve dnech 28. - 29. 12. 2015 stáhnul z PC záznamy hovorů, a to včetně hovoru ze dne 12. 1. 2016, tedy hovoru, který v té době nebyl ještě realizován (tvrzeno obžalobou)?

4) Lze zjistit, zda v průběhu vzdálenému přístupu realizovaného ve dnech 28. - 29. 12. 2015 (doba připojení v logu Teamviewer cca 5 minut) prokazatelně došlo ke zkopírování nahrávek telefonních hovorů?

5) V případě, že by obžalovaný chtěl skrýt vzdálený přístup z logu, mohl celý log vymazat? Případně ho úplně vypnout, aby o jeho vzdáleném přístupu nebyla jediná stopa? Existuje nějaký technický důvod, který by mu bránil se smazání celého logu?

6) Z hlediska posouzení IT odborníka, je technicky možný popis, jak to líčí poškozená (údajně viděla pohyb myši a stahování souborů z mobilu, který ale nebyl připojen a přesun do koše a vysypávání koše, stažení souborů z ledna 2016 již v prosinci 2015, dále poškozená neviděla žádné okno TeamViewer ani závěrečné okno, které by musela odkliknout) nebo je pravděpodobnější popis obžalovaného, kdy mu manželka nahrávky všech zájmových telefonátů předala osobně v lednu 2016?

7) Je možné získat ovládáním Teamviewer tímto poškozenou popsaným způsobem soubory z telefonu do PC užívaného poškozenou a pak, právě dle popisu „hýbala se myš a mazaly se soubory z koše"? Kam a jak by je mohl tímto popsaným způsobem obžalovaný kopírovat? Proč by se dostávaly vůbec do koše?

2 Nález

V průběhu cca tří týdnů jsem se vzrůstajícím údivem, co všechno se může stát, podrobně prostudoval celý trestní spis.

Tento znalecký posudek není klasickým výstupem zkoumání zajištěné techniky. Na položené otázky tedy mohu odpovědět pouze v teoretické rovině na základě své dvacetileté praxe soudního znalce s využitím informací z trestního spisu. Relevantních informací je však ve spise obsaženo velmi málo.
Veškeré zjištěné poznatky tak uvádím vždy pod textem každé jednotlivé otázky přímo v závěru tohoto posudku.

3 Závěr

1) **Je možné, aby komunikace mezi obžalovaným a poškozenou ze dne 19. 12. 2015 ohledně sepisu anonymního dopisu, předložená obžalovaným na elektronickém nosiči dat, byla zfalšována a případně jakým konkrétním způsobem?**

   V oblasti IT lze obecně teoreticky zfalšovat téměř vše. Není problém provést např. kopii komunikace do textového souboru a ten následně upravit standardním textovým editorem. U takto vytvořeného dokumentu (vzniklého exportem uložených zpráv) již nelze zjistit, zda k úpravám došlo nebo nikoli.

   Možnost falšování dat je obecně možná v situaci, kdy zdrojová data jsou uložena v zařízení, které je pod kontrolou osoby, která by takovéto falšování chtěla provést – to se týká např. lokálně (v počítači) uložených e-mailů, záznamů komunikátorů, uložených v mobilním telefonu (Viber, WhatsApp...). Pro pozměnění takovýchto informací v databázích jsou nutné velmi speciální znalosti, ovšem změny jsou možné a následným zkoumáním nelze zjistit, zda jsou data autentická nebo nikoli.

   Jiná situace je u informací, které jsou uloženy na serverech externí společnosti. V takovémto případě obecně nemá uživatel možnost tam uložené informace jakkoli modifikovat. Jedná se např. o zprávy, zaslané prostřednictvím sociální sítě Facebook nebo např. e-maily, umístěné na serverech některého z poskytovatelů e-mailových služeb (např. Seznam mail). Jakákoli modifikace takto uložených dat by byla možná pouze ve spolupráci s administrátory serverů výše uvedených společností.
   Zde by bylo možné po poskytnutí přihlašovacích údajů vytvořit např. znalecký posudek, kdy by soudem přibraný znalec provedl zadokumentování uložené komunikace.

2) **Jakým konkrétním způsobem by bylo možné zajistit dálkový přístup k počítači poškozené ve vztahu ke komunikaci (telefonátu) poškozené s policistou Kuncem?**

Mohu se vyjádřit pouze k možnostem zajištění vzdáleného přístupu k počítači obecně – specifický vztah k záznamu telefonátu zde z technického hlediska není.
Vzdálený přístup k počítači je možný mnoha způsoby, které se liší potřebou ovládání takového počítače. Pokud je vyžadováno kompletní přenesení obsahu obrazovky a ovládání počítače pomocí myši a klávesnice, existuje pro tento účel mnoho (desítek) programů. Namátkou mohu uvést CarbonCopy, PC Anywhere, VNC, Team Viewer nebo integrovanou součást operačního systému Windows – program Vzdálená plocha. Pokud je požadavek z ovládaného počítače např. pouze kopírovat soubory (bez nutnosti ovládání plochy počítače), je množství programů, které je možné použít ještě mnohem vyšší.

Pro použití mnoha z výše uvedených programů je nutné zajistit tzv. předávání portů na routeru – jedná se o onu malou krabičku, kterou mají mnozí doma – často je opatřena anténou a slouží k připojení zařízení k internetu prostřednictvím kabelu nebo WiFi.
V případě použití programu Vzdálená plocha, který je integrální součástí operačního systému Windows, by bylo nutné na routeru vytvořit tzv. VPN (šifrovaný tunel). K tomuto se mimo jiné vyjadřuje Jana Vlčková na listu č. 34 o servisním zásahu na jejím počítači: „*... technik přišel ke mně domů, vysvětlil mi, že ten router, který mám od manžela má vybudovaný tunel do mého PC. Pak mi ukazoval, že můj PC po zapnutí automaticky fotí obrazovku a snímky odesílá někam pryč. Dále mi řekl, že ten virus má schopnost číst znaky, které jsem namačkala na klávesnici. Dále zjistil, že mám on-line zapojenou i web kameru...*"

Toto je však v rozporu s vyjádřením p. Dušana Mlynka ze společnosti DIRECT DUTY Družstvo (listy 66 a 67), kdy tato společnost servisní zásah realizovala. Ve vyjádření této společnosti je uvedeno, že proběhl pouze úkon spočívající v přeinstalování počítače – tento nebyl ani spuštěn *(cituji: V prostředí Windows před recovery jsem nebyl. NTB byl prý neskutečně pomalý, takže jsem zálohu dat provedl externím nástrojem, který běží rychle nezávisle na samotném OS, takže netuším, zda se tam něco dělo na pozadí.)*

3) **Jsou při ohledání zjištěné vzdálené přístupy do počítače ve dnech 28. 12. a 29. 12. 2015 pouze torzem původních informací o dálkovém přístupu, mohly být informace o dálkovém přístupu z počítače reálně vymazány? Lze vyloučit, že vzdálený přístup do počítače poškozené a stažení záznamu telefonátu poškozené s policistou Kuncem mohlo být učiněno kdykoli přede dnem 28. 12. a 29. 12. 2015?**

Záznamy o připojení se k počítači prostřednictvím programu Team Viewer pocházejí z tzv. logu – souboru, do nějž si program samotný ukládá informace o své činnosti. V době zkoumání počítače kpt. Ing. Mračnem, které proběhlo 18. července 2016 bylo zjištěno, že tento program byl v minulosti odinstalován. K odinstalaci programu muselo dojít mezi 29. 12. 2015 (poslední zaznamenané použití programu) a 21.1.2016 (tento den proběhlo přeinstalování počítače p.

Vlčkové externí firmou (str. 66 spisu), kdy v okamžiku přeinstalace již musel být program odinstalován – zachoval se pouze právě onen log o záznamu činnosti programu. Při odinstalování totiž tento program smaže všechny svoje soubory a komponenty, záznam o činnosti (log) ale nechává nedotčený. Faktem je, že od 29. 12. 2015 do okamžiku (nejpozdějšího) dne odinstalace dne 21. 1. 2016 vzdálené připojení k počítači prostřednictvím tohoto programu neproběhlo.

Vzhledem k tomu, že se v logu programu Team Viewer zachovaly pouze záznamy o dvou připojeních, předpokládám, že se nejedná o kompletní záznam. Po instalaci programu je obvykle provedena minimálně zkouška spojení a ověření funkčnosti připojení. Vzhledem k tomu, že jakákoli informace o dřívějším připojení chybí, lze předpokládat, že došlo ke smazání dřívějšího logu. Toto smazání může provést přímo uživatel počítače (fyzicky u něj sedící) nebo uživatel připojený vzdáleně pomocí libovolného programu pro vzdálené ovládání – i při připojení samotným programem Team Viewer. Připojení k počítači před 28. 12. 2015 tak bylo možné a při smazání logu programu by o tomto nezůstaly zachovány žádné informace.

4) Mohlo dojít k dálkovému přístupu k počítači poškozené a stažení výše uvedeného telefonátu jiným způsobem?

Jak jsem již uvedl, k dálkovému přístupu k počítači mohlo teoreticky dojít prostřednictvím mnoha nejrůznějších programů. Problémem je, že při ohledání počítače policejním orgánem (listy 133 až 135) nebyly žádné takové programy zjištěny. Nebylo např. ani zadokumentováno, zda bylo povoleno vzdálené ovládání prostřednictvím integrovaného nástroje operačního systému Windows Vzdálená plocha.
Nemohu se ztotožnit se závěrem ohledání věci (list 134), kde je uvedeno: *„...Pokud by se však v počítači nacházel nějaký profesionální špionážní program, jeho nalezení by bylo prakticky nemožné...".*
Právě naopak – pokud by byly v průběhu ohledání počítače zadokumentovány procesy, automaticky spouštěné při startu systému, lze následnou analýzou těchto vybraných procesů jednoznačně stanovit, zda se jedná o software pro vzdálenou správu nebo nikoli.

Pokud přistoupíme na myšlenkovou konstrukci, že cílem obžalovaného bylo kopírovat z počítače p. Vlčkové soubory, nepochybně existují různé způsoby, kterými toto lze zajistit – často mnohem „elegantnější" než použití programu Team Viewer, kdy při každém vzdáleném připojení je na obrazovce počítače zobrazeno hlášení o připojení a jsou jasně viditelné veškeré operace.
Celým spisem se táhne jako červená nit, že pan obžalovaný má nadstandardní znalosti v oblasti IT. Dokážu si představit, že ideálním způsobem, jak zajistit kopírování souborů z počítače p. Vlčkové by mohla být např. instalace jednoduchého FTP serveru (při přesměrování portů na routeru). To by umožnilo (z hlediska uživatelky počítače) naprosto neodhalitelný přístup k notebooku. Uvedených způsobů vzdáleného přístupu k počítači existují desítky – výše uvedený příklad je pouze jeden z mnoha.

Z hlediska stažení záznamu telefonátu je nutné prohlásit, že aby bylo možné soubor z počítače zkopírovat vzdáleně na jiný počítač, je nutné, aby se tento soubor již nacházel na disku počítače – jinak by nebylo co kopírovat. Lze teoretizovat o tom, že p. Vlčková ponechala připojený telefon prostřednictvím kabelu k počítači. V takovém to případě by mohl vzdálený uživatel počítače (za podmínky, že by použil některý z programů, umožňující vzdálené ovládání počítače na úrovni plochy) přistoupit k datům telefonu a data zkopírovat z telefonu na pevný disk počítače. Následně by jej mohl zkopírovat do počítače svého.
Budeme-li předpokládat, že ke vzdálenému připojení byl použit program Team Viewer – informace o použití jiného programu jsou v rovině spekulací – muselo by k tomuto dojít v době před 28. 12. 2015 (poslední zaznamenané připojení před odinstalací programu) za předpokladu, že došlo ke smazání logu o činnosti programu Team Viewer před tímto datem.

5) **Jak by vzdálený přístup do počítače mohl být osobou používající počítač vnímán v intencích toho, co vypovídá poškozená?**

V případě vzdáleného přístupu prostřednictvím programu pro kompletní vzdálené řízení počítače (Team Viewer a další programy, uvedené výše) dochází k „přesměrování" klávesnice a myši. Uživatel, který se fyzicky nachází u ovládaného počítače tak vidí všechny úkony, které se na počítači dějí, tak, jako by obsluhoval svoji myš a klávesnici. V praxi je možné používat jak lokální klávesnici a myš, tak i klávesnici a myš vzdálenou. Je např. možné otevřít textový editor, napsat několik slov, další slova může napsat vzdálený uživatel... Počítač se chová tak, jako by k němu byly připojeny dvě klávesnice a myši. Pohledem na obrazovku tak lze pozorovat veškeré operace, které se na počítači dějí.
Pokud by byl na počítači aktivní program pro kopírování souborů (např. FTP server), vzdálené připojení se nijak neprojeví a uživatel, nacházející se u počítače nemá žádnou možnost zjistit, že k připojení došlo.

6) **Jakým způsobem by obžalovaný mohl s ohledem na pohyb mobilních přístrojů poškozené a obžalovaného (viz úřední záznam na č.l. 333 a násl. spisu) postupovat v případě, že by se mělo jednat o fingovanou textovou zprávu? Bylo by možné přihlášení na mobilní telefon poškozené v místě buňky jejího bydliště v době, kdy ho měl mít údajně obžalovaný?**

Jakým způsobem by mohl obžalovaný postupovat, aby odeslal textovou zprávu z telefonu p. Vlčkové v 9:01 v Odolené Vodě na svůj telefon, kterou přijal v 9:35 v Praze v Opletalově ulici opravdu nevím.
Jak vyplývá ze záznamů o uskutečněném telekomunikačním provozu (listy 119 – 122), telefon p. Vlčkové se v době odeslání zprávy nacházel v blízkosti vysílače mobilního signálu Větrná 304, Odolená Voda. Mohlo by se spekulovat o scénáři, že p. obžalovaný odeslal v 9:01 zprávu z telefonu p. Vlčkové v Odolené Vodě, telefon zanechal na místě a následně zběsile ujížděl do Prahy (cesta dle internetových vyhledávačů trvá za mírného provozu 27 minut). Tam

by zapnul svůj telefon (před tím prokazatelně vypnutý) a zprávu přijal. Tento scénář nekoresponduje s výpovědí p. Vlčkové, která uvedla, že její telefon jí byl odňat p. obžalovaným a následně navrácen v odpoledních hodinách. Ze záznamů telekomunikačního provozu je přitom zřejmé, že telefon p. Vlčkové neopustil Odolenou Vodu minimálně do času 14:14. Z dalších záznamů naopak vyplývá, že telefon obžalovaného se od 10:00 dále připojoval k mobilní síti výhradně v Praze a v místě jeho trvalého bydliště.

Telefonní přístroj se připojuje k buňce mobilního vysílače, která je mu geograficky nejbližší, resp. k té, u níž má zajištěnu nejlepší úroveň signálu. Je zcela vyloučeno, aby se mobilní telefon, nacházející se např. v Praze připojil k vysílači v Odolené Vodě.

Poslední poznámka se týká vyjádření policejního orgánu na č.l. 334 – cituji: „*Ve věci je nutno vyzdvihnout podezřelou okolnost a sice to, že mobilní telefon, užívaný obviněným, který se mu v důsledku vybití měl sám vypnout, tak po připojení do el. zásuvky vozidla mu umožňoval okamžitý a téměř soustavný provoz, spočívající v několikaminutových telefonních hovorech, v přijímání a odesílání SMS zpráv a automatickém přihlašování k internetu.*"

Ačkoli úplně nevím, jak to souvisí s vyšetřovanou věcí, v rámci objektivity bych chtěl poznamenat, že na této skutečnosti mě osobně nepřipadá podezřelé vůbec nic. V každém případě závisí na kvalitě (resp. výstupním nabíjecím proudu) autonabíječky. Pokud je zcela vybitý telefon připojen k nabíječce, do několika desítek sekund až minut je možné jej zapnout a běžně jej používat.

7) Uveďte další skutečnosti, které považujete za podstatné z hlediska své znalecké odbornosti.

Veškeré relevantní informace jsem již uvedl v odpovědích na předchozí otázky

Ve znaleckém posudku je dále třeba posoudit a odpovědět na tyto otázky obžalovaného:

1) Existují jakékoliv technické podklady, ze kterých se lze důvodně domnívat, že záznamy telefonních hovorů se vůbec někdy nacházely na PC obžalovaného, užívaného poškozenou? Jsou pro tuto domněnku jakékoliv technické stopy? Uveďte které.

Žádné informace o tom, že by se na disku počítače nacházely záznamy telefonních hovorů se v trestním spise nevyskytují. V dokumentu „Protokol o ohledání věci" (č.l. 134) je pouze uvedeno: „*...V uživatelských datech se poté nachází fotografie (i smazané), smazané filmy, dokumenty a další data.*"

Z uvedené citace vyplývá, že součástí úkonu bylo i provedení obnovy dříve smazaných dat. Předpokládám, že kdyby se na disku počítače předmětné nahrávky hovorů vyskytovaly buď jako existující soubory nebo jako soubory smazané, které by byly rekonstruovány v průběhu obnovy dat, bylo by to v protokolu uvedeno.

2) **Pokud existují záznamy na PC obžalovaného, užívaného poškozenou o existenci záznamů telefonních hovorů, existují jakékoliv technické stopy směřující k domněnce, že tyto zájmové soubory na PC nahrál obžalovaný?**

Viz odpověď na otázku č. 1

3) **Lze zjistit, zda obžalovaný ve dnech 28. - 29. 12. 2015 stáhnul z PC záznamy hovorů, a to včetně hovoru ze dne 12. 1. 2016, tedy hovoru, který v té době nebyl ještě realizován (tvrzeno obžalobou)?**

Z dochovaného záznamu o připojení nelze identifikovat, jaké činnosti byly na počítači prováděny. Pokud byl záznam hovoru vytvořen dne 12. 1. 2016, pak je vcelku logické, že nemohl být kýmkoli zkopírován před tím, než vůbec vznikl.

4) **Lze zjistit, zda v průběhu vzdálenému přístupu realizovaného ve dnech 28. - 29. 12. 2015 (doba připojení v logu Teamviewer cca 5 minut) prokazatelně došlo ke zkopírování nahrávek telefonních hovorů?**

Z dochovaného záznamu nelze zjistit, jaké činnosti byly na počítači realizovány.

5) **V případě, že by obžalovaný chtěl skrýt vzdálený přístup z logu, mohl celý log vymazat? Případně ho úplně vypnout, aby o jeho vzdáleném přístupu nebyla jediná stopa? Existuje nějaký technický důvod, který by mu bránil se smazání celého logu?**

Soubor s logem (záznamem o činnosti programu Team Viewer) lze smazat. Technický důvod, který by bránil jeho smazání, není.

6) **Z hlediska posouzení IT odborníka, je technicky možný popis, jak to líčí poškozená (údajně viděla pohyb myši a stahování souborů z mobilu, který ale nebyl připojen a přesun do koše a vysypávání koše, stažení souborů z ledna 2016 již v prosinci 2015, dále poškozená neviděla žádné okno TeamViewer ani závěrečné okno, které by musela odkliknout) nebo je pravděpodobnější popis obžalovaného, kdy mu manželka nahrávky všech zájmových telefonátů předala osobně v lednu 2016?**

Z pochopitelných důvodů se nemohu vyjádřit ve smyslu, že mě přijde pravděpodobnější verze ta či ona.
Výpověď p. Vlčkové z technického hlediska působí poněkud chaoticky – nemohu ovšem posoudit, jak záznam výpovědi zcela přesně odpovídá ji vnímané realitě. Je zřejmé, že ve výše popsané otázce jsou popsány skutečnosti, které z technického hlediska nastat nemohou – kopie dat z telefonu, který není připojen k počítači, resp. kopírování souborů před tím, než byly fyzicky vytvořeny.

7) **Je možné získat ovládáním Teamviewer tímto poškozenou popsaným způsobem soubory z telefonu do PC užívaného poškozenou a pak, právě dle popisu „hýbala se myš a mazaly se soubory z koše"? Kam a jak by je mohl tímto popsaným způsobem obžalovaný kopírovat? Proč by se dostávaly vůbec do koše?**

Jak již jsem uvedl, při připojení programem Team Viewer není rozdíl mezi tím, zda uživatel fyzicky sedí u počítače a používá jeho myš a klávesnici nebo zda používá klávesnici a myš, vzdálenou tisíce kilometrů. Pokud někdo bude na počítači přesouvat soubory do koše, uvidí osoba sedící u obrazovky pohyb myši i všechny související činnosti.
Pro kopírování souborů do vzdáleného počítače slouží samostatná část programu Team Viewer. S mazáním souborů, resp. jejich přesunem do koše to samozřejmě nemá nic společného.

4 Znalecká doložka

Znalecký posudek byl zpracován ve dnech 5. 4. 2018 – 3. 5. 2018.
Technické úkony byly realizovány pracovníky znalecké kanceláře.
Posudek je vyhotoven v pěti kopiích – Výtisk č. 1, 2, 3 a 4 pro Okresní soud Praha-východ, Na Poříčí 1044/20, 112 97 Praha 1; Výtisk č. 5 (bez příloh) pro archiv znalce.
Znalecký posudek jsem podal jako znalec, jmenovaný rozhodnutím Krajského soudu Praha, nám. Kinských 5, ze dne 14. 10. 1999, spr. 4049/98, pro obory:

- Kybernetika, odvětví Výpočetní technika
- Elektronika, odvětví Elektronika, specializace Bezpečnost informačních systémů

Znalecký úkon je zapsán pod pořadovým číslem 4165 znaleckého deníku.

Znalec si je vědom následků vědomě nepravdivého znaleckého posudku.

Znalečné a náhradu nákladů účtuji podle připojené likvidace.

Ing. Jan Janka

Ing. JAN JANKA
soudní znalec
Elektronika