Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Martin Vašek** **Oponent:** **Ing. Jiří Hološka, Ph.D.**

Studijní program:	**Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Akademický rok:	**2012/2013**
Téma diplomové práce:	**Využití forenzních metod pro odhalování počítačové kriminality a ochranu dat v kyberprostoru**

Student si vybral mimořádně náročné o obsáhlé téma, útoky v kyberprostoru běžně nabývají různých forem je nutné tuto problematiku řešit v širších souvislostech. Student obecně zpracoval problematiku forenzní analýzy s ohledem na českou legislativu, bez ohledu na zbytek světa popřípadě alespoň na legislativu v Evropské unii. Student se pokusil shrnout základní principy, bohužel nedbral v potaz technický detail který je očekáván od studenta při zpracování diplomové práce. Veškeré informace jsou předkládány v teoretické rovině s minimálním přesahme do praktického použití. Je zřejmé že ačkoliv student čerpal z kvalitních zdrojů, pokud tak lze usuzovat ze seznamu literatury uvedeného v diplomové práci, měl problém s podstatou přebíraných informací. Diplomová práce je tak plná neúplných nebo zkreslených informací.

Po formální stránce je diplomová práce velice slabá zejména z jazykového hlediska. V práci je množství vět které nedávají smysl, nebo si protiřečí, práce obsahuje výrazy v cizích jazycích, nejspíše pocházející z informačních zdrojů , které student neuvádí. Student v práci velice špatně pracuje s literaturou, v seznamu literatury je uvedeno dvacet tři zdrojů, nicméně v textu diplomové práce je citováno pouze sedm zdrojů. První citace je uvedena na straně dvanáct a je citován zdroj číslo osm, další citace se nachází až na straně dvacet čtyři, kde je citován zdroj číslo pět, zdroj číslo jedna je citován na straně šedesátšest atd.

Obsahová část práce má značné nedostatky zejména v technickém detailu předkládaných informací. Student si měl vybrat specifickou část forenzní analýzy a té se dále detailně věnovat. Bohužel to student neučinil a snažil se do práce zahrnout veškeré činnosti které spadají do forenzní analýzy a řízení incidentů. Výsledkem je teoretická část která značně zasahuje i do praktické části které se student téměř nevěnoval.

V praktické části student zmínil několik zajímavých témat, které mohly být rozebrány do větší podrobnosti. Konkrétně se jedná o analýzu časových značek a forenzní analýzu mobilních telefonů. Na tyto témata budou primárně zaměřeny doplňující otázky k obhajobě.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Poprosil bych studenta krátkou a poutavou formou zodpovědět následující otázky:

1) **V kapitole 8.3.4.1 Postup použití HW ochrany proti zápisu uvádíte „*k znaleckému počítači připojíme originální datové nosiče pro ochranu proti zápisu*“, můžete vysvetlit co jste tím myslel ?**
2) **V praktické části využíváte komerční nástroje např. od fy. Elcomsoft, můžete nastínit podmínky za kterých jste prováděl testování na těchto nástrojích ?**
3) **Obrázek 31, výpis metadat souborového systému pro analýzu časových značek. Z obrázku není patrné pro jaké časové pásmo je analýza zpracována, můžete krátce nastínit jak aplikace řeší problematiku časových pásem ? Tz. zda aplikace používá aktuálně nastavené časové pásmo na forenzním počítači, nebo zda je možné definovat časovou zónu ručně.**
4) **V práci neuvádíte způsoby změn metadat souborových systému v závislosti na souborových operacích. Můžete krátce pohovořit o změnách časových značek pro souborové systémy FAT32 a NTFS při kopírování a přesouvání souborů ?**
5) **V kapitole 8.6.1 se věnujete duplikaci GSM SIM karet, umožňuje takto vytvořený duplikát karty přístup do GSM sítě, nebo slouží pouze k překonání SIM locku na mobilním telefonu ?**
6) **Pokud jste na předchozí otázku odpovědel, že klon SIM umožňuje přístup do GSM sítě, poprosil bych Vás o nastínění procesu jakým způsobem se zvolený nástroj vyrovnává s ochranou před klonováním v podobě čítače omezujicího počet autentizačních cyklů SIM karty.**

Práci doporučuji k obhajobě.

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

D - uspokojivě.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 10.6.2013

Podpis oponenta diplomové práce