



## Agenda szkolenia „Certyfikowany Informatyk Śledczy” poziom średniozaawansowany

### Dzień I

Czas	Temat	Prowadzący
8:00-8:10	Rejestracja Sprawy organizacyjne	
8:10-10:10	Źródła potencjalnych dowodów elektronicznych - przegląd Fizyczna i logiczna budowa dysków twardych - przypomnienie Co to jest „slack space”? - pliki - dysk logiczny - dysk fizyczny Co to jest „unallocated space”? Informatyka śledcza - Metodyka przeprowadzania badania	Paweł Babski
10:10:10:20	Przerwa kawowa	
10:20-12:20	„Elektroniczne ślady” pozostawiane przez systemy plików: - FAT - NTFS Odtwarzanie usuniętych partycji z dysków Identyfikacja śladów usuwania danych i defragmentacji - odtwarzanie skasowanych danych - wpływ defragmentacji na usunięte dane	Paweł Babski
12:20-13:00	Lunch	
13:00-15:00	Analiza plików Microsoft Office - MS Office – pliki tymczasowe („temp files”) - MS Office – metadane o dokumentach i „śledzenie zmian” („track changes”)	Paweł Babski
15:00-15:10	Przerwa	
15:10-17:10	Komunikatory internetowe (GaduGadu, ICQ i inne) - identyfikacja programów i analiza logów Wykorzystanie Internetu jako narzędzia śledczego, m.in. - Google - Arin - WHOIS	Paweł Babski



## Dzień II

Czas	Temat	Prowadzący
8:00-10:00	<b>MS Windows – ślady w systemie</b> <ul style="list-style-type: none"><li>- "link files"</li><li>- Systemowy "kosz" (Recycle Bin)</li><li>- Katalog systemowy "Prefetch"</li></ul>	<b>Grzegorz Idzikowski</b>
10:00-10:10	<b>Przerwa kawowa</b>	
10:10-12:10	<b>Poczta elektroniczna</b> <ul style="list-style-type: none"><li>- główne systemy pocztowe i standardowe formaty</li><li>- klienci – Outlook, Lotus Notes, Eudora, Netscape, GroupWise</li><li>- serwery – Exchange, Groupwise, SendMail, Domino</li></ul>	<b>Grzegorz Idzikowski</b>
12:10-12:50	<b>Lunch</b>	
12:50-14:50	<b>Analiza poczty elektronicznej</b> <ul style="list-style-type: none"><li>- Paraben Email Examiner</li><li>- Konwersja MS Outlook OST na PST</li><li>- Odtwarzanie skasowanych maili (PST)</li><li>- pliki NSF (Lotus Notes)</li><li>- poczta internetowa</li></ul>	<b>Grzegorz Idzikowski</b>
14:50-15:00	<b>Przerwa</b>	
15:00-17:00	<b>Przeglądarki internetowe</b> <ul style="list-style-type: none"><li>- Internet Explorer (Cache, plik historii, ustawienia, zakładki, OWA)</li><li>- Mozilla/Firefox (Cache, Settings, Mail, Bookmarks)</li></ul>	<b>Grzegorz Idzikowski</b>



### Dzień III

Czas	Temat	Prowadzący
8:00-10:00	<b>Wyszukiwanie danych wg słów kluczowych</b> <ul style="list-style-type: none"><li>- koncepcja „słów kluczowych”</li><li>- ograniczanie wolumenu wyników przez wykorzystanie funkcji GREP</li></ul>	<b>Grzegorz Idzikowski</b>
10:00-10:10	<b>Przerwa kawowa</b>	
10:10-12:10	<b>Aplikacje do niszczenia danych (<i>Wiping tools</i>)</b> <ul style="list-style-type: none"><li>- identyfikacja programów</li><li>- identyfikacja śladów</li></ul> <b>Analiza rejestrów systemu Windows – przydatne ślady</b> <ul style="list-style-type: none"><li>- instalowane oprogramowanie</li><li>- podłączone nośniki zewnętrzne</li><li>- historia wizyt WWW</li><li>- inne</li></ul>	<b>Grzegorz Idzikowski</b>
12:10-13:00	<b>Lunch</b>	
13:00-15:00	<b>Wstęp do zabezpieczania i analizy zawartości pamięci RAM</b> <ul style="list-style-type: none"><li>- Podstawowe metody wykonywania „obrazu” pamięci RAM w systemach Windows i Linux</li><li>- Analiza artefaktów w pamięci RAM – wprowadzenie</li></ul>	<b>Grzegorz Idzikowski</b>
15:00-15:20	<b>Podsumowanie i zakończenie szkolenia</b>	<b>Grzegorz Idzikowski</b>

Jest to ramowy plan szkolenia. Czas poszczególnych bloków tematycznych może się nieznacznie zmienić, wydłużyć lub skrócić np.: w zależności od trudności tematu.

W związku z czym prosimy o elastyczne potraktowanie czasu wyznaczonego dwugodzinnymi blokami.