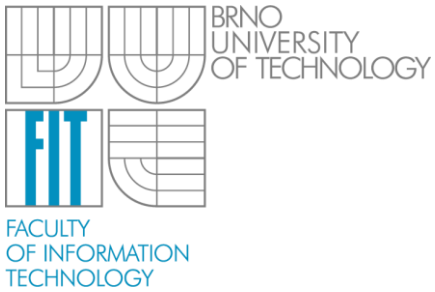
# Sec6Net Content Visualization

Rudolf Kajan, Michal Zachariáš

Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 2, 612 66 Brno
ikajanr@fit.vutbr.cz
izacharias@fit.vutbr.cz




9.12.2013

# Vizualizace

Hlavním cílem vizualizačního bloku je přehledné a intuitivní zobrazování zachycených dat, umožňující vytvořit si komplexní obraz o komunikaci v čase a napříč různými protokoly.

Vizualizační blok přímo navazuje na rekonstrukční blok, což v důsledku znamená, že výstupy rekonstrukčního bloku (XML soubor s meta-informacemi, které popisují komunikaci jednotlivých uživatelů pomocí protokolů, a zachycené binární data) jsou přímými vstupy bloku vizualizačního

# Požadavky na vizualizační nástroj

Samotné implementaci předcházela důkladná analýza požadavků kladených na vizualizační nástroj. Jako stěžejní požadavky byly identifikovány především následující:

- Přehledné a názorné zobrazení zachycených dat a jejich efektivní filtrování.
- Jednoduchá rozšiřitelnost v oblasti podpory protokolů.
- Podpora vlastních vizualizačních komponent a dynamicky generovaného grafického uživatelského rozhraní.
- Efektivní manipulace a filtrace velkého množství záznamů.
- Podpora přehrávání širokého spektra audio a video formátů.

Jednoduchá instalace – zbavení se závislostí na knihovnách třetích stran, jedinou prerekvizitou je přítomnost .NET Frameworku 4.0.

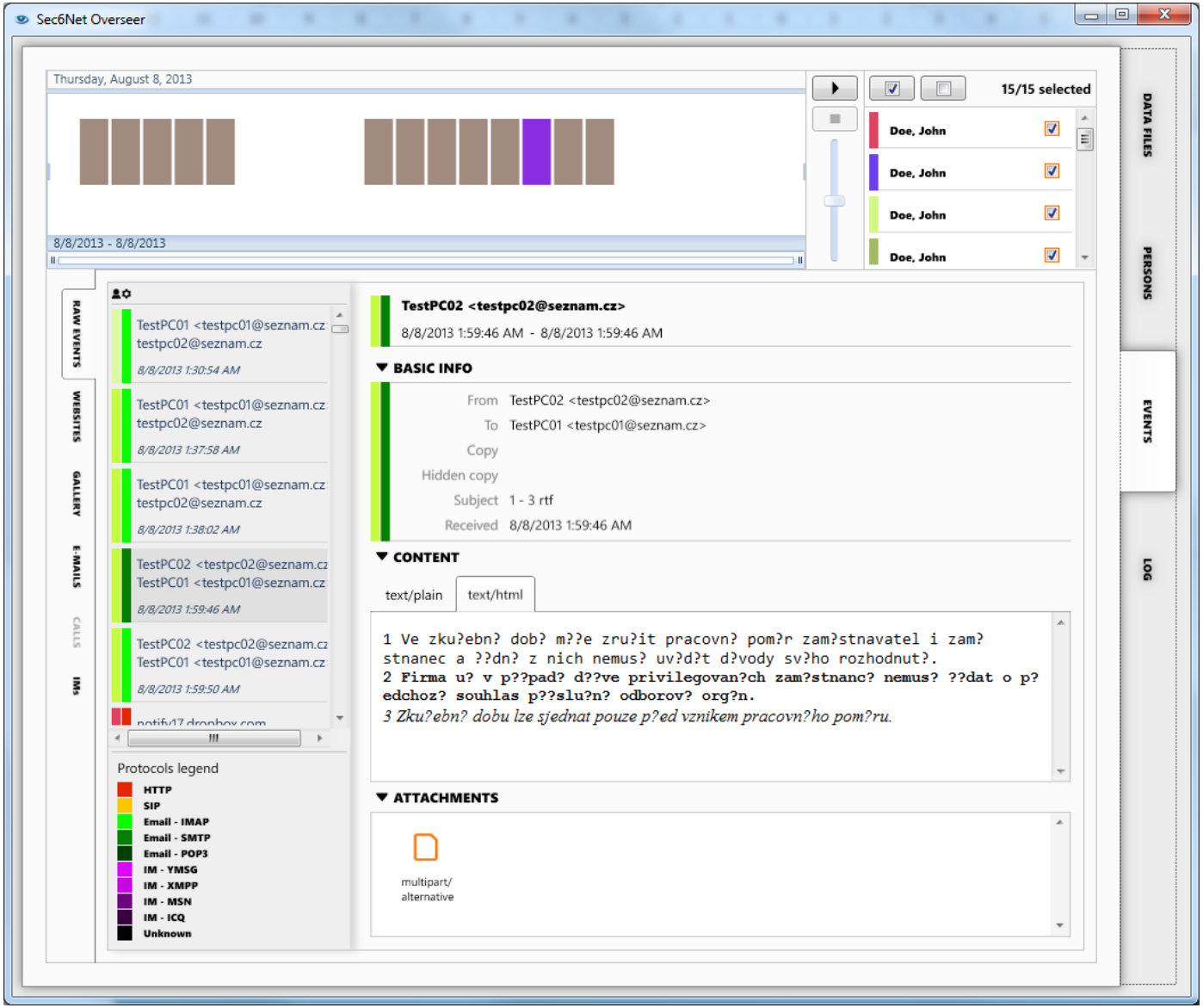
# Způsoby vizualizace

Data jsou vizualizována pomocí tzv. pohledů. Každý pohled se skládá alespoň z jedné komponenty, která zobrazuje určité aspekty zpracovaných dat, např. komponenta zobrazující metadata fotografií nebo komponenta zobrazující IM zprávy v čase. Při návrhu těchto komponent byl kladen velký důraz na jejich znovupoužitelnost v různých pohledech a jejich snadnou nahraditelnost v případě změny struktury dat.

Kvůli velkým rozdílům mezi jednotlivými protokoly, není vhodné používat jediný generický datový pohled. Zanikly by tak detaily komunikace. Například v Instant Messagingu je důležité, aby si uživatel jasně uvědomil časový rámec komunikace a identitu komunikujících stran.

Po načtení dat z vybraného datového zdroje je zvolen úvodní pohled, který zobrazuje veškerou komunikaci (podobně jako Wireshark). Do tohoto pohledu se načítá komunikace z entit nezávisle na typu protokolu a detailech konkrétních událostí. Pohled ukazuje hlavní události každého protokolu, například žádost o zobrazení webové stránky pro HTTP nebo zahájení a ukončení hovoru pro H.323.

# Hlavní okno aplikace



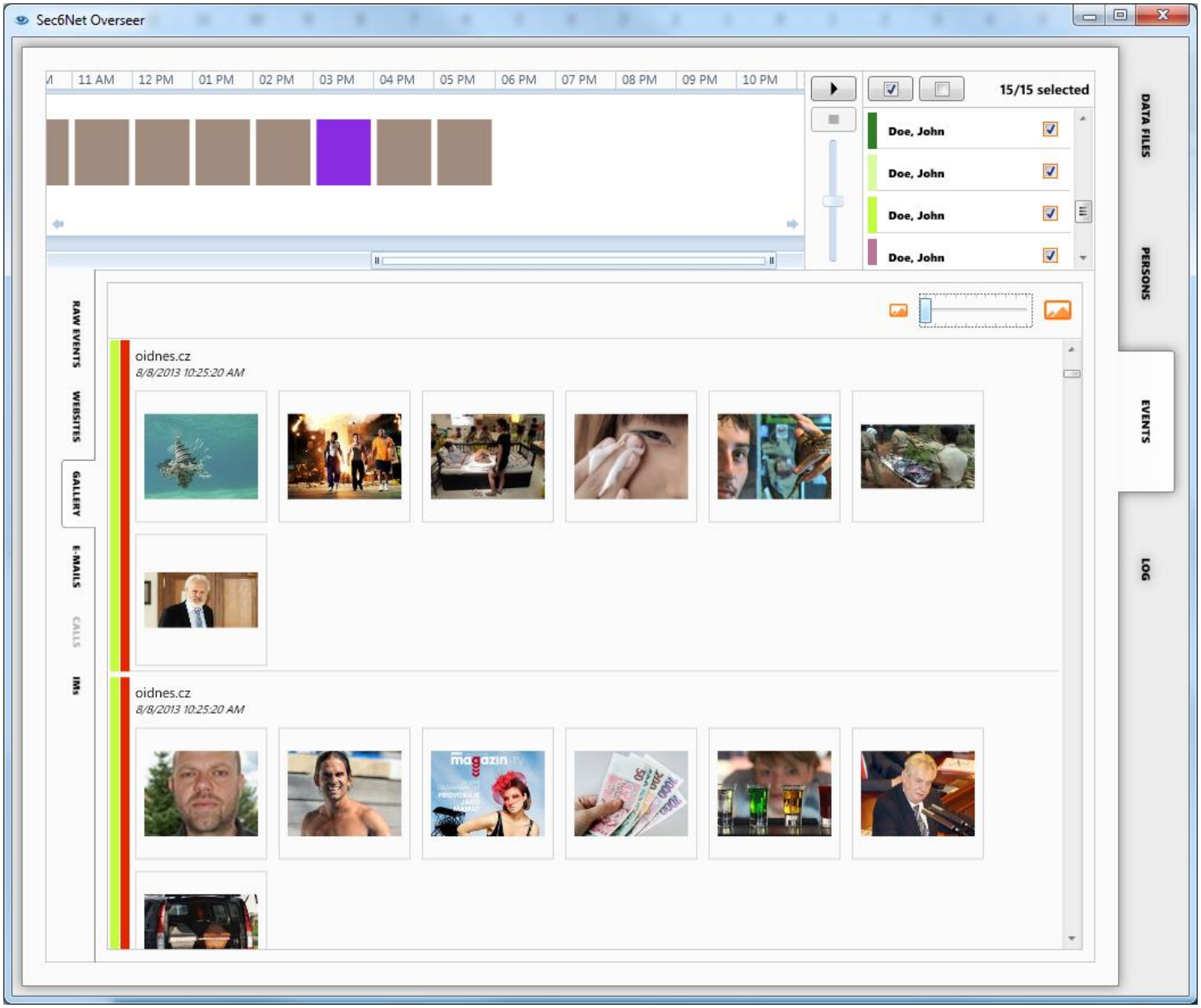
# Filtrování

Aplikace dokáže zpracovávat a vizualizovat velké množství dat. Z důvodu přehlednosti je nutné data filtrovat a vybírat jen ta, která jsou pro uživatele v daný moment relevantní. Vizualizační nástroj pro každý pohled poskytuje možnost filtrování na základě:

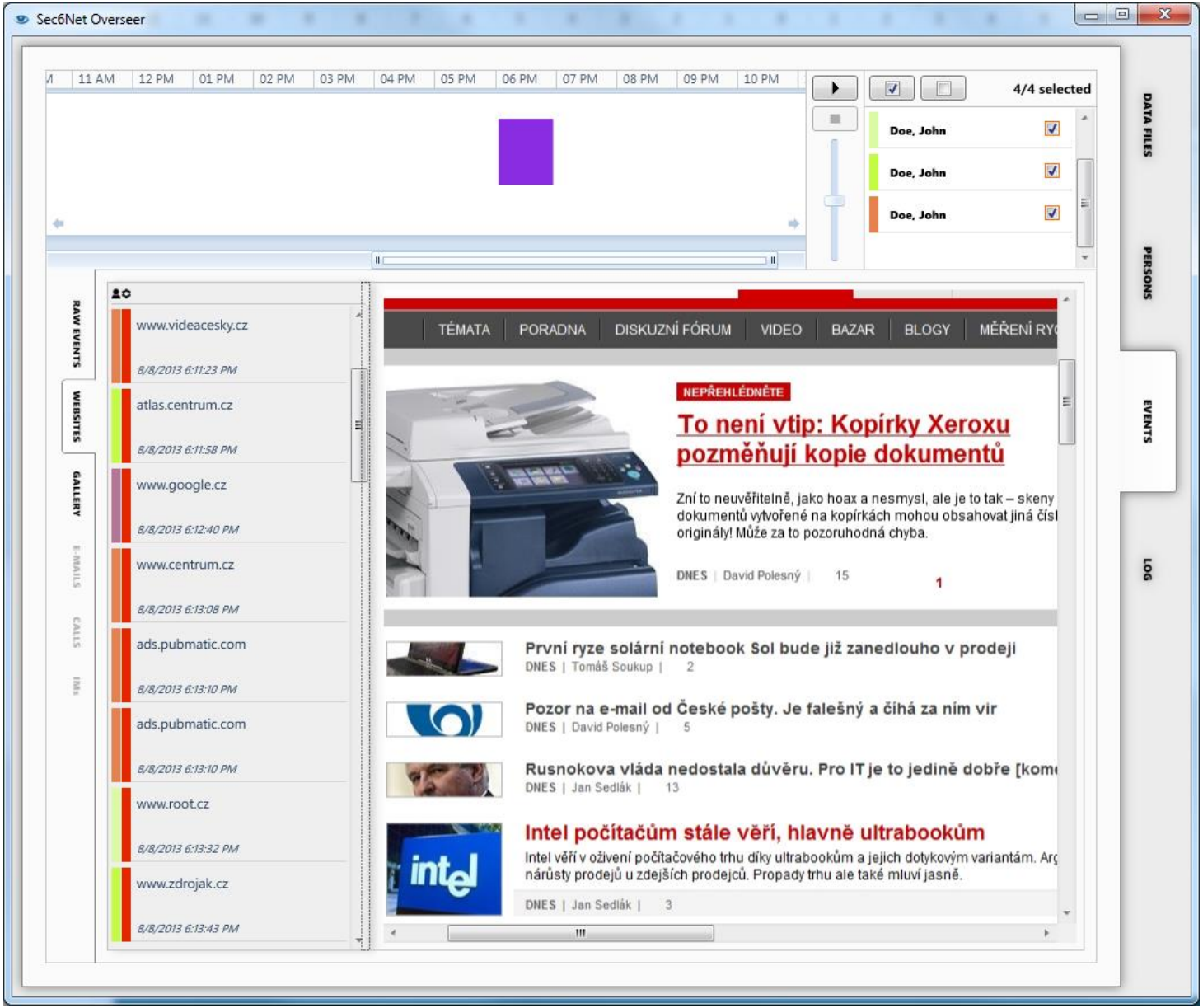
- předdefinovaných filtrovacích výrazů (email, adresa, telefonní číslo, rodné číslo apod.)
- uživatelem nadefinovaných vzorů pomocí regulárních výrazů

Pro zajištění rychlosti a paměťové efektivity bylo filtrování implementováno pomocí kombinace lambda výrazů a dynamických funkcí, jejichž vykonávaní je automaticky optimalizováno na úrovni .NET Frameworku.

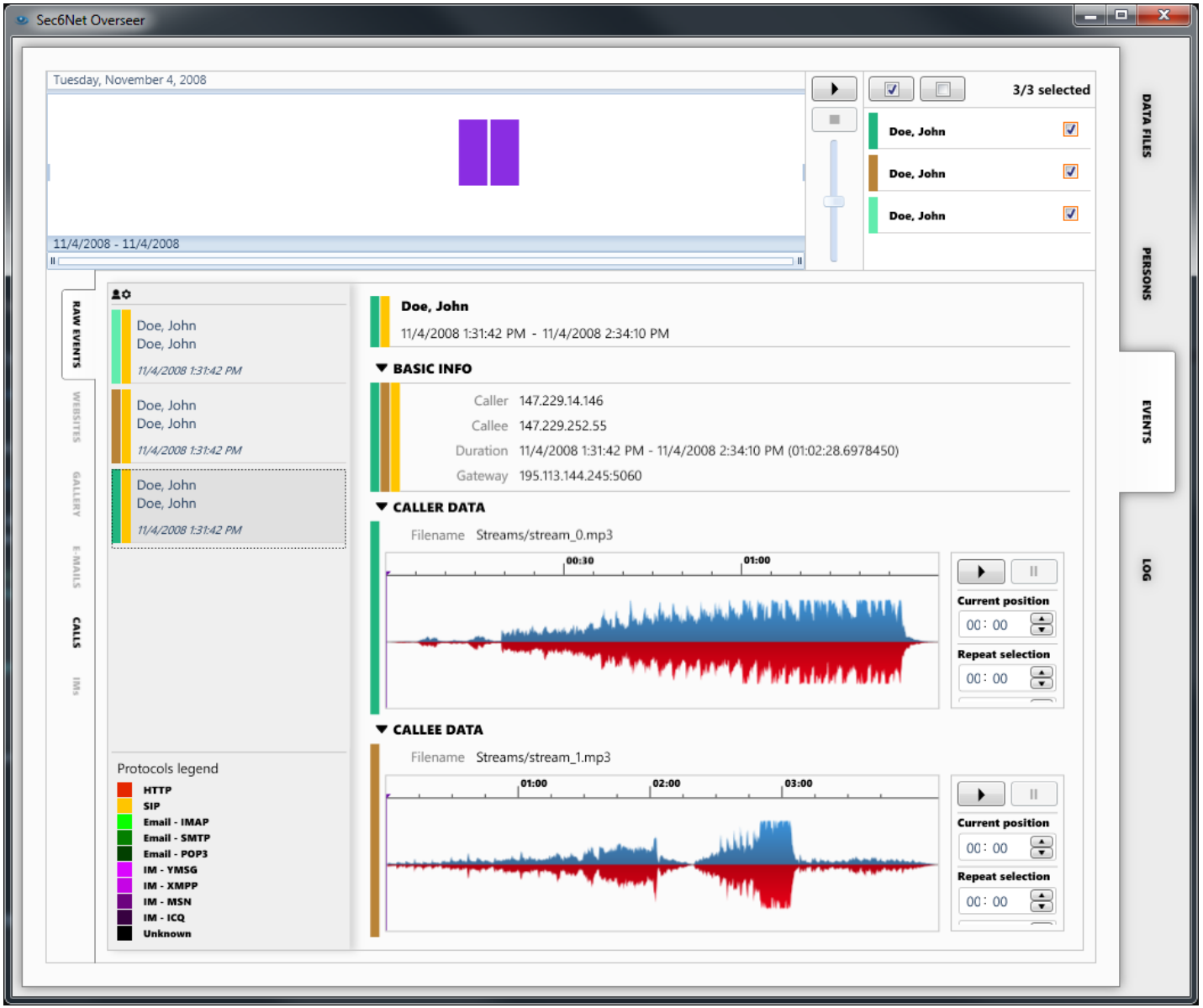
# Pohled na zachycené obrázky



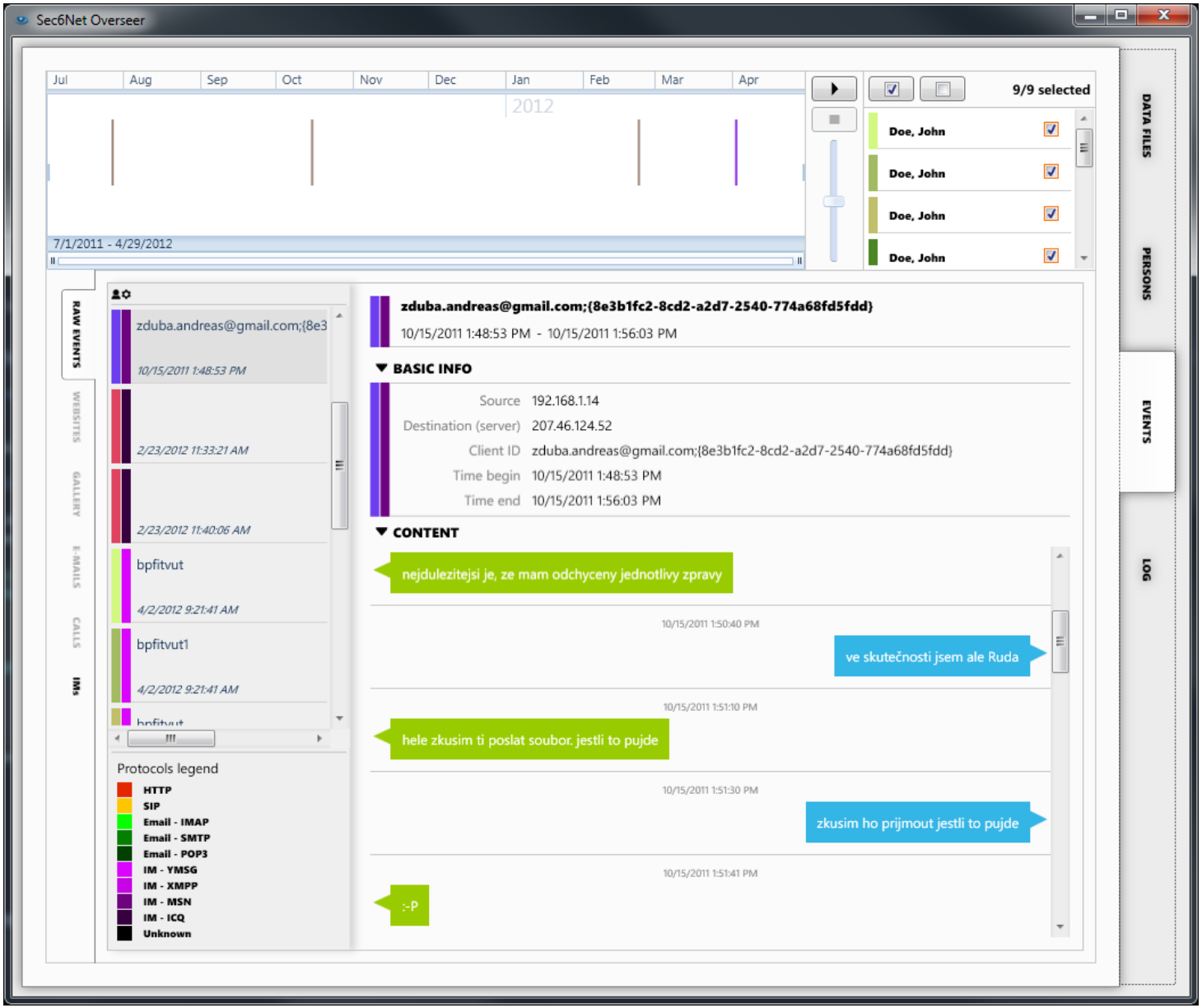
# Pohled na rekonstruované webové stránky



# Pohled na Skype hovory



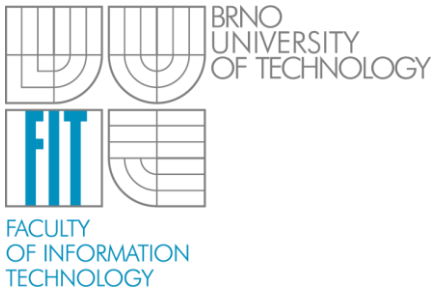
# Pohled na IM konverzace



# Sec6Net Content Visualization

Rudolf Kajan, Michal Zachariáš

Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 2, 612 66 Brno
ikajanr@fit.vutbr.cz
izacharias@fit.vutbr.cz




9.12.2013