

# Sec6Net Content Visualization

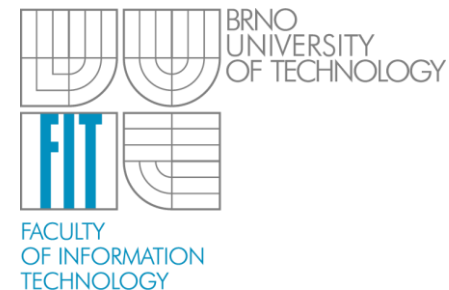
Rudolf Kajan, Michal Zachariáš

Vysoké učení technické v Brně, Fakulta informačních technologií

Božetěchova 2, 612 66 Brno

ikajanr@fit.vutbr.cz

izacharias@fit.vutbr.cz



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

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

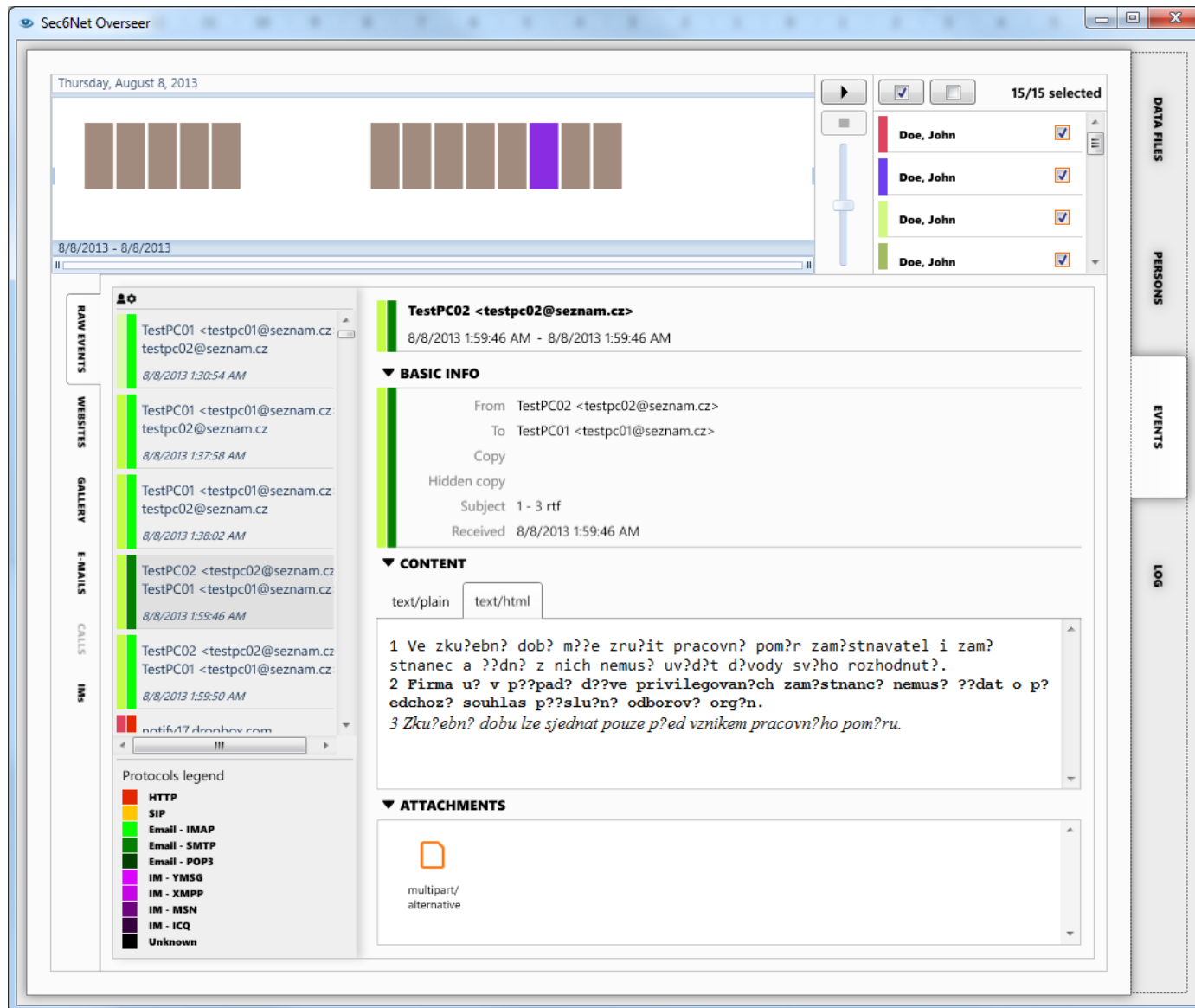
- Přehledné a názorné zobrazení zachycených dat a jejich efektivní filtrování.
- Jednoduchá rozšiřitelnost v oblasti podpory protokolů.
- Podpora vlastních vizualizačních komponent a dynamicky generovaného grafického uživatelského rozhraní.
- Efektivní manipulace a filtrace velkého množství záznamů.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

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.

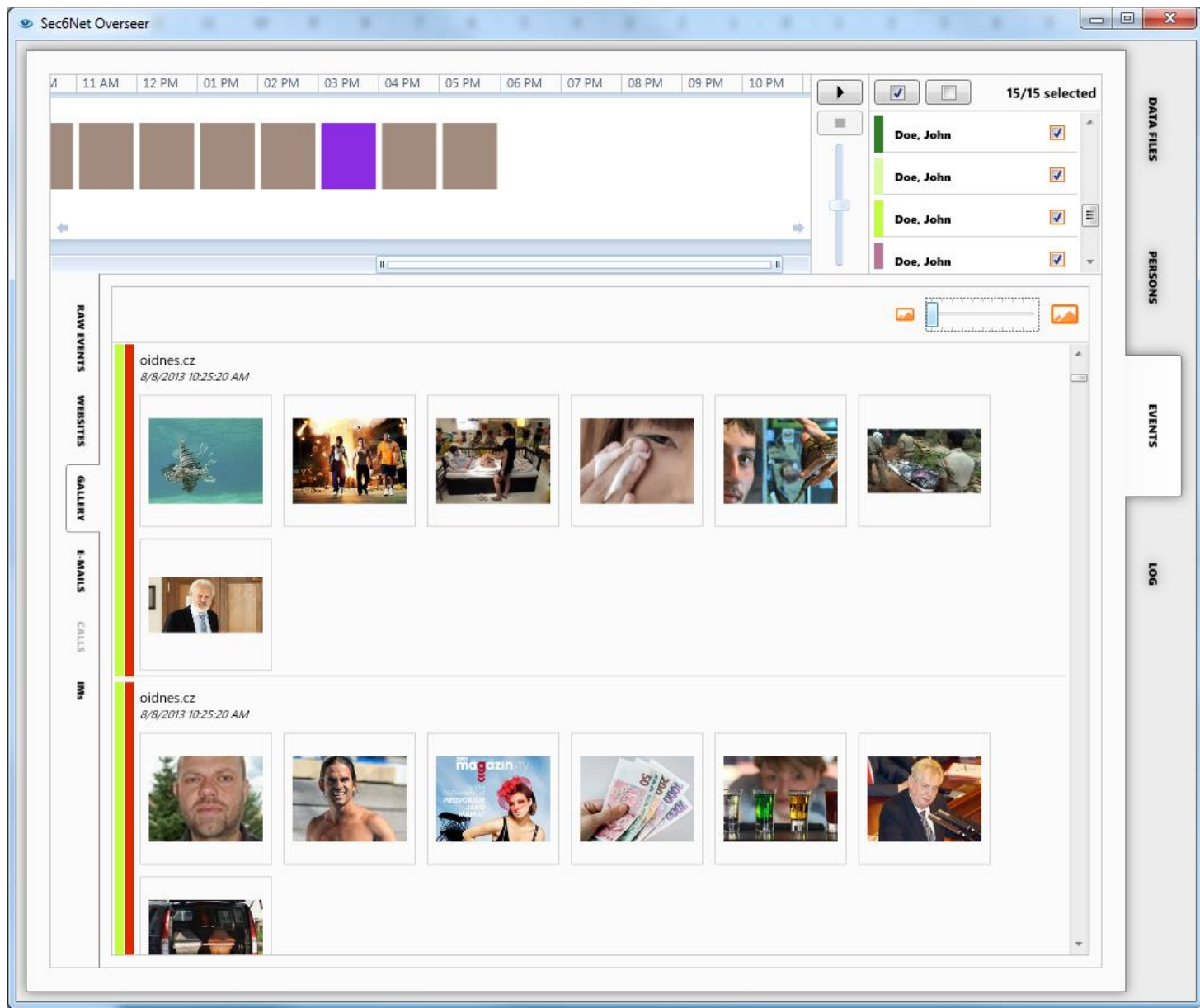


Aplikace dokáže zpracovávat a vizualizovat velké množství dat. Z důvodu přehlednosti je nutné data filtrovat a vybírat jen ta, která jsou pro uživatele v daný moment relevantní. Vizualizační nástroj pro každý pohled poskytuje možnost filtrování na základě:

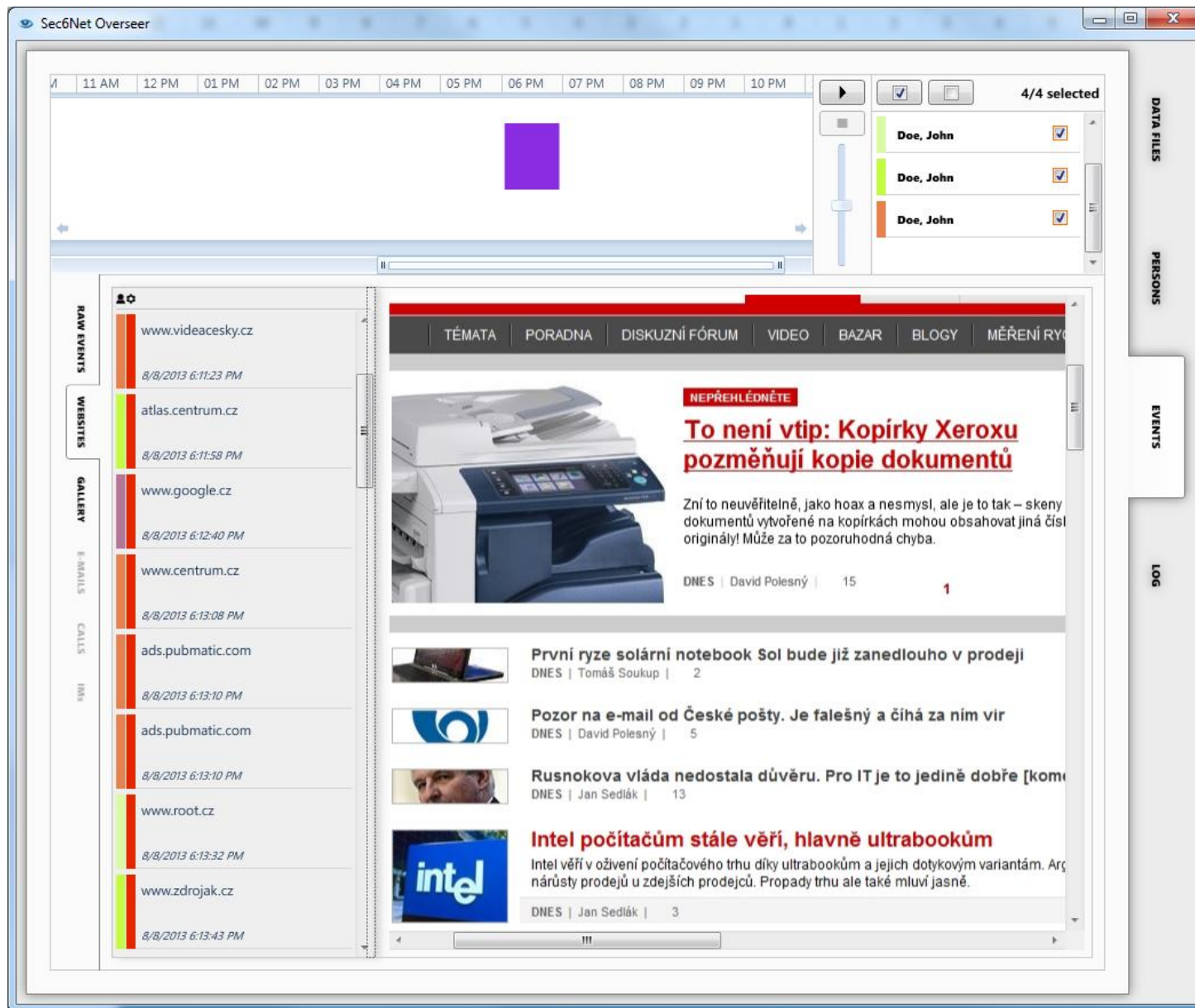
- předdefinovaných filtrovacích výrazů (email, adresa, telefonní číslo, rodné číslo apod.)
- uživatelem nadefinovaných vzorů pomocí regulárních výrazů

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

# Pohled na zachycené obrázky







The screenshot displays the Sec6Net Overseer application window. The main area shows a reconstructed website with a red header and a navigation menu. The website content includes a featured article about Xerox copiers and several news snippets. On the left, a sidebar lists various data sources like RAW EVENTS, WEBSITES, GALLERY, E-MAILS, CALLS, and IMs. On the right, a panel shows selected data files and persons.

**Sec6Net Overseer**

Time: 11 AM, 12 PM, 01 PM, 02 PM, 03 PM, 04 PM, 05 PM, 06 PM, 07 PM, 08 PM, 09 PM, 10 PM

4/4 selected

**DATA FILES**

- Doe, John
- Doe, John
- Doe, John

**PERSONS**

**EVENTS**

**LOG**

**RAW EVENTS**

- www.videacesky.cz  
8/8/2013 6:11:23 PM
- atlas.centrum.cz  
8/8/2013 6:11:58 PM
- www.google.cz  
8/8/2013 6:12:40 PM
- www.centrum.cz  
8/8/2013 6:13:08 PM
- ads.pubmatic.com  
8/8/2013 6:13:10 PM
- ads.pubmatic.com  
8/8/2013 6:13:10 PM
- www.root.cz  
8/8/2013 6:13:32 PM
- www.zdrojak.cz  
8/8/2013 6:13:43 PM

**WEBSITES**

**GALLERY**

**E-MAILS**

**CALLS**

**IMs**

**TÉMATÁ** **PORADNA** **DISKUZNÍ FÓRUM** **VIDEO** **BAZAR** **BLOGY** **MĚŘENÍ RY**

**NEPŘEHLEDNĚTE**

**To není vtip: Kopírky Xeroxu pozměňují kopie dokumentů**

Zní to neuvěřitelně, jako hoax a nesmysl, ale je to tak – skeny dokumentů vytvořené na kopírkách mohou obsahovat jiná čísla originály! Může za to pozoruhodná chyba.

DNES | David Polesný | 15

**První ryze solární notebook Sol bude již zanedlouho v prodeji**

DNES | Tomáš Soukup | 2

**Pozor na e-mail od České pošty. Je falešný a číhá za ním vir**

DNES | David Polesný | 5

**Rusnokova vláda nedostala důvěru. Pro IT je to jediné dobře [komentář]**

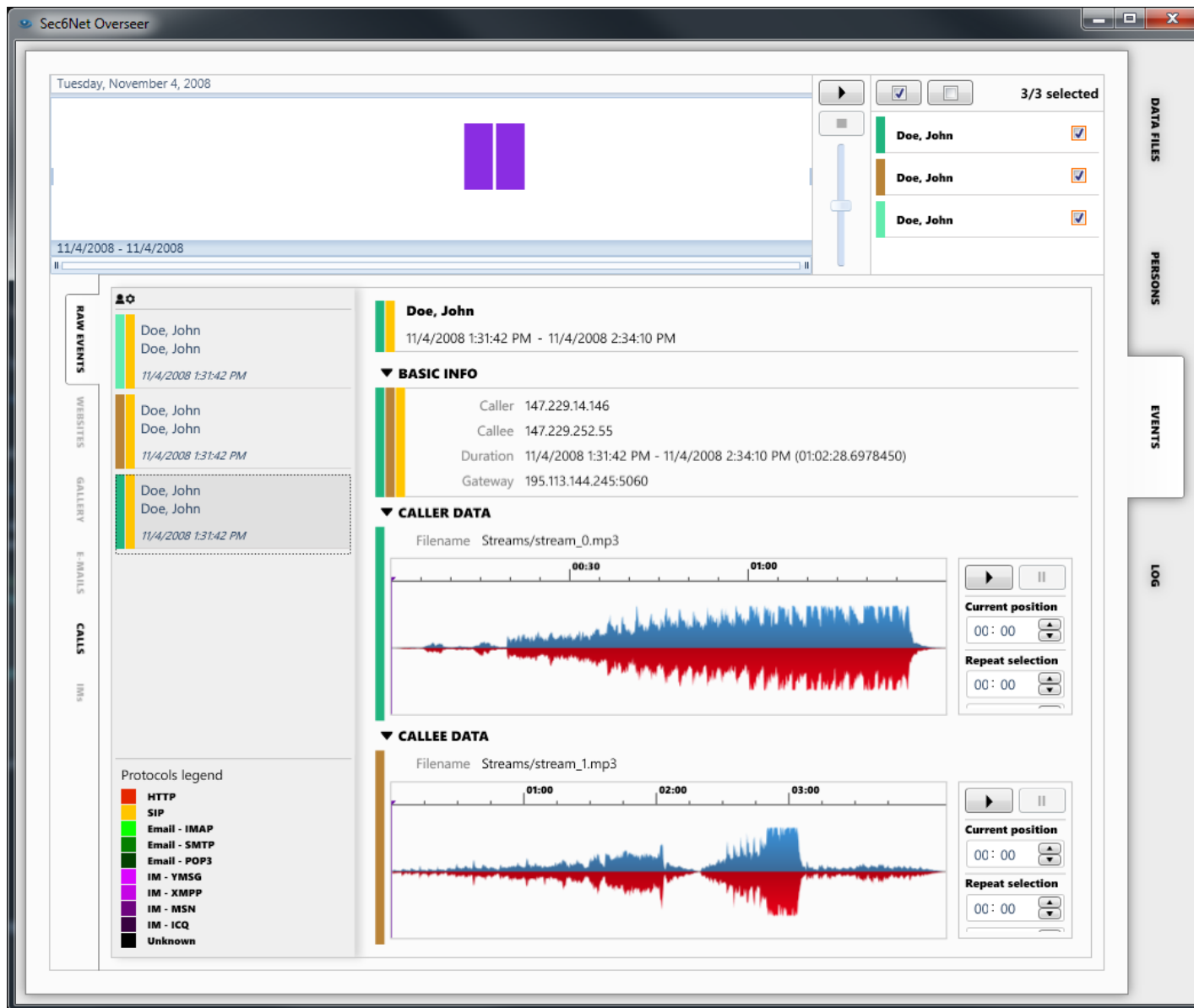
DNES | Jan Sedláček | 13

**Intel počítačům stále věří, hlavně ultrabookům**

Intel věří v oživení počítačového trhu díky ultrabookům a jejich dotykovým variantám. Arg nárůsty prodeje u zdejších prodejců. Propady trhu ale také mluví jasně.

DNES | Jan Sedláček | 3





Sec6Net Overseer

Tuesday, November 4, 2008

11/4/2008 - 11/4/2008

3/3 selected

- ☒ Doe, John
- ☒ Doe, John
- ☒ Doe, John

**RAW EVENTS**

- Doe, John  
Doe, John  
11/4/2008 1:31:42 PM
- Doe, John  
Doe, John  
11/4/2008 1:31:42 PM
- Doe, John  
Doe, John  
11/4/2008 1:31:42 PM

**PROTOCOLS LEGEND**

- HTTP
- SIP
- Email - IMAP
- Email - SMTP
- Email - POP3
- IM - YMSG
- IM - XMPP
- IM - MSN
- IM - ICQ
- Unknown

**Doe, John**  
11/4/2008 1:31:42 PM - 11/4/2008 2:34:10 PM

**BASIC INFO**

- Caller 147.229.14.146
- Callee 147.229.252.55
- Duration 11/4/2008 1:31:42 PM - 11/4/2008 2:34:10 PM (01:02:28.6978450)
- Gateway 195.113.144.245:5060

**CALLER DATA**

Filename Streams/stream\_0.mp3

00:30 01:00

Current position 00:00

Repeat selection 00:00

**CALLEE DATA**

Filename Streams/stream\_1.mp3

01:00 02:00 03:00

Current position 00:00

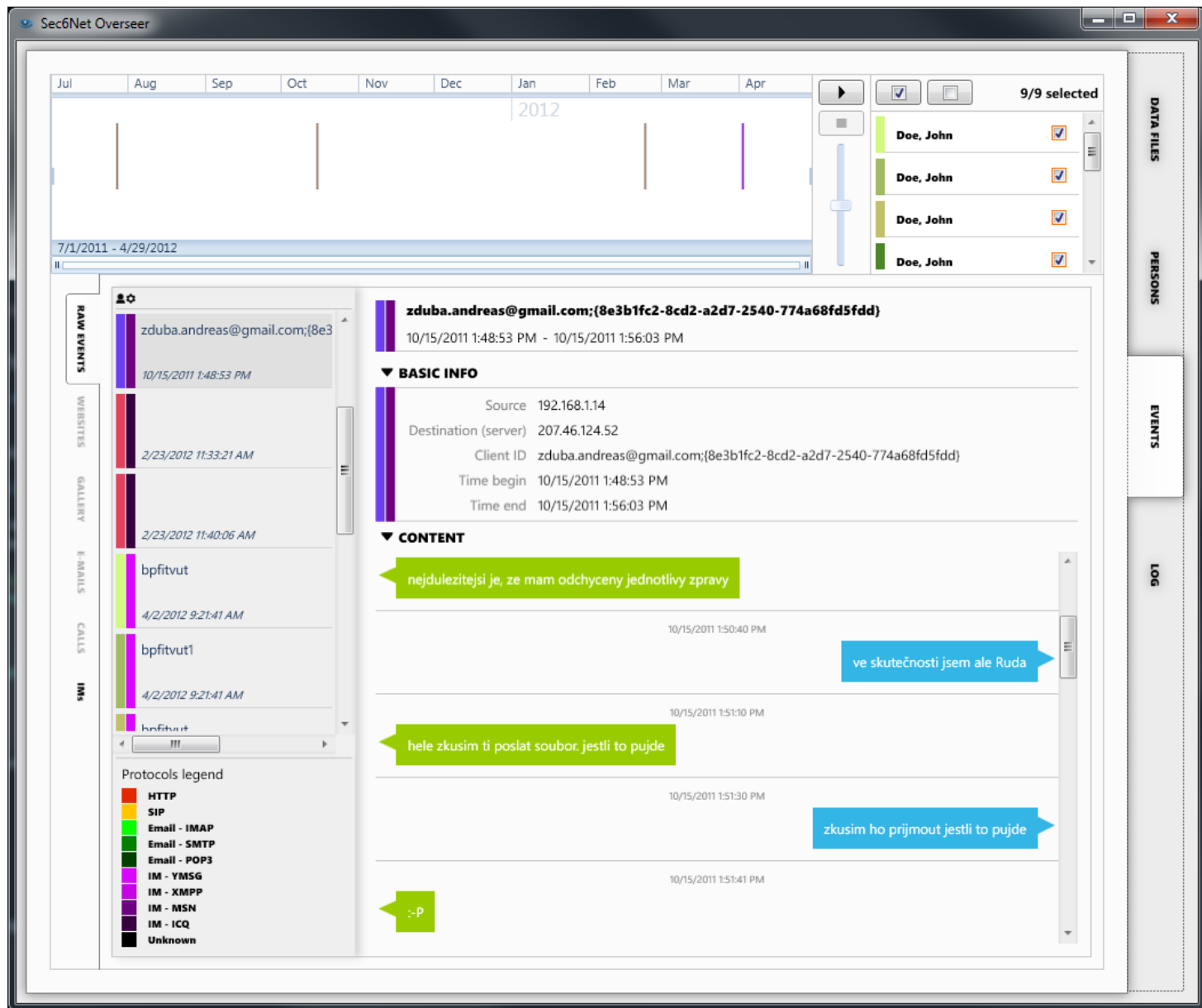
Repeat selection 00:00

**DATA FILES**

**PERSONS**

**EVENTS**

**LOG**



The screenshot displays the Sec6Net Overseer application window. The top navigation bar includes a calendar for 2012 (Jul to Apr) and a list of 9/9 selected contacts, all named "Doe, John". The left sidebar contains a "RAW EVENTS" list with entries for "zduba.andreas@gmail.com;{8e3b1fc2-8cd2-a2d7-2540-774a68fd5fdd}" and a "PROTOCOLS LEGEND" for various protocols like HTTP, SIP, Email-IMAP, etc. The main pane shows a detailed view of an IM conversation with "zduba.andreas@gmail.com;{8e3b1fc2-8cd2-a2d7-2540-774a68fd5fdd}" on 10/15/2011. The conversation includes a "BASIC INFO" section with source, destination, and client ID, and a "CONTENT" section with several messages in Czech. The messages are: "nejdulezitejsi je, ze mam odchyceny jednotlivy zpravy", "ve skutečnosti jsem ale Ruda", "hele zkusim ti poslat soubor. jestli to pujde", and "zkusim ho prijmout jestli to pujde". The interface also features a "DATA FILES", "PERSONS", "EVENTS", and "LOG" sidebar on the right.

Sec6Net Overseer

Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr 2012

7/1/2011 - 4/29/2012

9/9 selected

Doe, John

Doe, John

Doe, John

Doe, John

RAW EVENTS

zduba.andreas@gmail.com;{8e3b1fc2-8cd2-a2d7-2540-774a68fd5fdd}

10/15/2011 1:48:53 PM

2/23/2012 11:33:21 AM

2/23/2012 11:40:06 AM

bpfitvut

4/2/2012 9:21:41 AM

bpfitvut1

4/2/2012 9:21:41 AM

bpfitvut

PROTOCOLS legend

- HTTP
- SIP
- Email - IMAP
- Email - SMTP
- Email - POP3
- IM - YMSG
- IM - XMPP
- IM - MSN
- IM - ICQ
- Unknown

▼ BASIC INFO

Source 192.168.1.14

Destination (server) 207.46.124.52

Client ID zduba.andreas@gmail.com;{8e3b1fc2-8cd2-a2d7-2540-774a68fd5fdd}

Time begin 10/15/2011 1:48:53 PM

Time end 10/15/2011 1:56:03 PM

▼ CONTENT

nejdulezitejsi je, ze mam odchyceny jednotlivy zpravy

10/15/2011 1:50:40 PM

ve skutečnosti jsem ale Ruda

10/15/2011 1:51:10 PM

hele zkusim ti poslat soubor. jestli to pujde

10/15/2011 1:51:30 PM

zkusim ho prijmout jestli to pujde

10/15/2011 1:51:41 PM

:-P

DATA FILES

PERSONS

EVENTS

LOG

# 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

