Belkasoft
forensics made easier

3724 Heron Way, Palo Alto CA 94303 USA
+1 (650) 272-03-84 (USA and Canada)
+7 (812) 926-64-74 (Europe and other regions)

DONALD C. COPELAND, DIGITAL & CYBER FORENSICS, USA

About Digital & Cyber Forensics LLC

Donald is a forty year veteran of the computer industry and CEO of Digital & Cyber Forensics LLC. His firm provides comprehensive forensic support in areas such as civil proceedings & disputes, criminal proceedings, corporate espionage, cyber attacks, e-Discovery, and more.

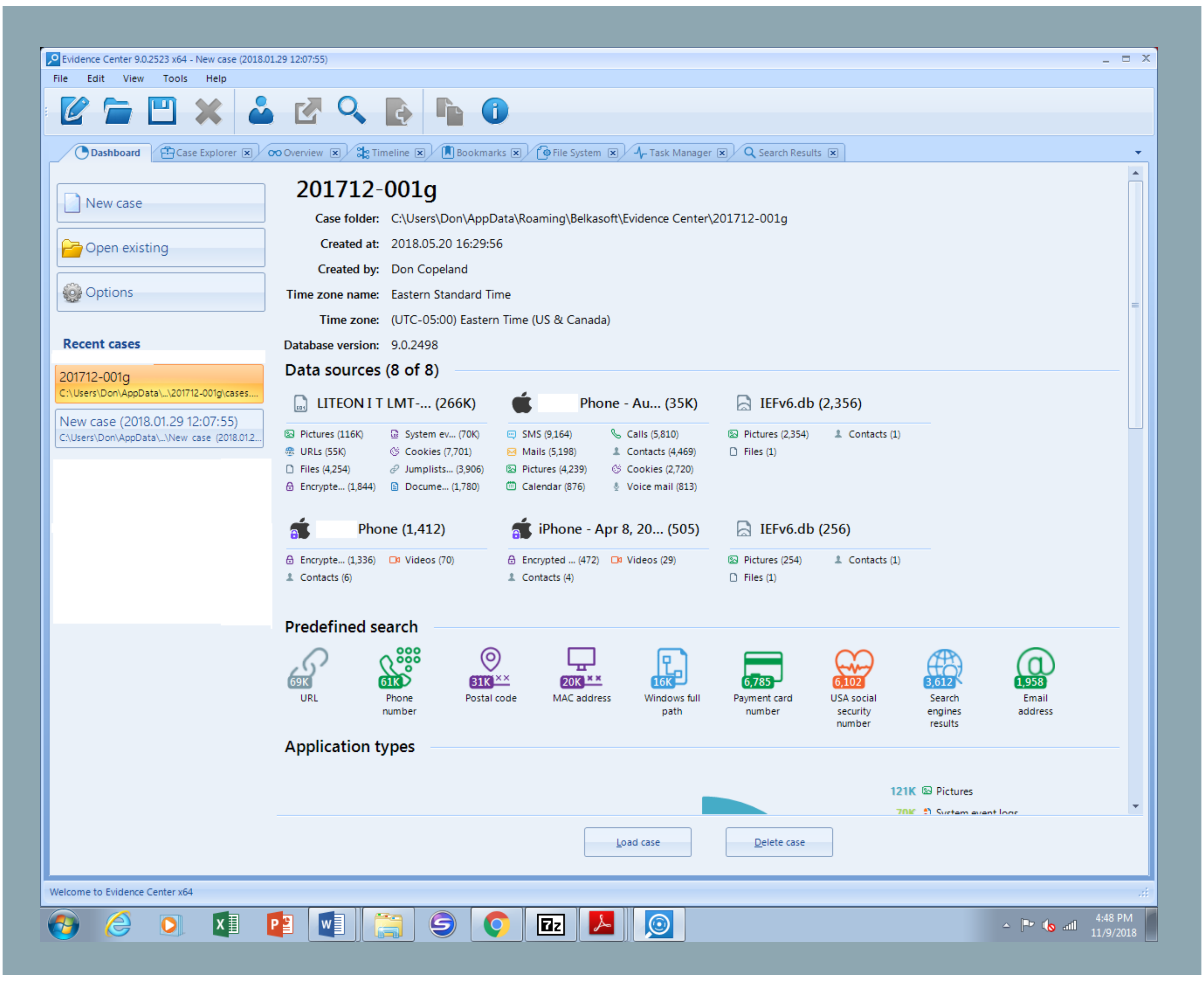
Donald uses various forensic tools in his line of work, trying to keep the balance between functionality and cost. He chose BEC for the case he describes below because artifact detection was his top priority and Belkasoft is one of the best tools for that.

About the case

There is an old saying in life: "A picture is worth a thousand words." That's what I received, instantly, when I ingested E01 files from a 256GB SSD drive on a particular case. I was working with a client on this case and was already familiar with many of the files and data that was associated with the drive. Much of the analysis was very simple and clear, however there were deeper issues still to be uncovered.

> *"The functionality, performance and value far exceed the cost!"*

I followed my normal process and ingested the image into Belkasoft Evidence Center. Immediately when it was finished, I received the screen shown below. Without even beginning to determine what I had to deal with, I saw multiple data sources. This was very important here due to the nature of the case, it included sources acquired from backups of Apple iPhones which had been connected to iTunes on the drive.



Evidence Center 9.0.2523 x64 - New case (2018.01.29 12:07:55)

Recent cases

201712-001g
C:\Users\Don\AppData\...\201712-001g\cases....

New case (2018.01.29 12:07:55)
C:\Users\Don\AppData\...\New case (2018.012...

201712-001g

Case folder: C:\Users\Don\AppData\Roaming\Belkasoft\Evidence Center\201712-001g
Created at: 2018.05.20 16:29:56
Created by: Don Copeland
Time zone name: Eastern Standard Time
Time zone: (UTC-05:00) Eastern Time (US & Canada)
Database version: 9.0.2498

Data sources (8 of 8)

LITEON I T LMT-... (266K)
Pictures (116K) · System ev... (70K)
URLs (55K) · Cookies (7,701)
Files (4,254) · Jumplists... (3,906)
Encrypte... (1,844) · Docume... (1,780)

[redacted] Phone - Au... (35K)
SMS (9,164) · Calls (5,810)
Mails (5,198) · Contacts (4,469)
Pictures (4,239) · Cookies (2,720)
Calendar (876) · Voice mail (813)

IEFv6.db (2,356)
Pictures (2,354) · Contacts (1)
Files (1)

[redacted] Phone (1,412)
Encrypte... (1,336) · Videos (70)
Contacts (6)

iPhone - Apr 8, 20... (505)
Encrypted ... (472) · Videos (29)
Contacts (4)

IEFv6.db (256)
Pictures (254) · Contacts (1)
Files (1)

Predefined search

URL	Phone number	Postal code	MAC address	Windows full path	Payment card number	USA social security number	Search engines results	Email address
69K	61K	31K	20K	16K	6,785	6,102	3,612	1,958

Application types

121K Pictures
70K System event logs

As mentioned earlier, there were deeper issues still to be uncovered! When drilling down in the file system, low and behold there were "spindump" files associated with cell phone crashes. These backup data from the cell phones provided detailed information as to what happened on two phones during two separate instances. Needless to say, when you're trying to connect the dots with facts in order to find the truth, every element of precision detail is important.

I went on to use other functionally provided by the application. The product was very easy to use, I probably shouldn't say that, but to move around in the application with ease provided for a great degree of comport and confirmed findings from the other applications as well. I make it a habit in forensic examinations not to rely on only one product. There is that "Trust but Verify" here.

In a previous business venture, I would tell people: "You're getting proportionate quality for price!" I believe this saying has been overcome here by Belkasoft. "The functionality, performance and value far exceed the cost!"