Credits:
Gavriloaie Eugen-Andrei (shiretu@gmail.com)(http://www.rtmpd.com/)
Luke Kenneth Casson Leighton (lkcl@lkcl.net)(http://lkcl.net/)

Client chunk 1 (first 1536 bytes)

Start	Stop	length	Semnification	Zone name
0	3	4	uptime	A
4	7	4	version	B
8	11	4	digest offset	C
12	12+digest offset-1	digest offset	Unknown zone	D
12+digest offset	12+digest offset+31	32	digest	E
12+digest offset+32	739	696-digest offset	Unknown zone	F
740	771	32	Unknown zone	G
772	772+dh offset -1	dh offset	Unknown zone	H
772+dh offset	772+dh offset+127	128	dh	I
772+dh offset+128	1403	504-dh offset	Unknown zone	J
1404	1531	128	Unknown zone	K
1532	1535	4	dh offset	L

A: I always put it 0

B: Impersonate with 9.0.124.2 (4 bytes: 9,0,124,2)

C: the bytes in this zone gives the offset to the digest with the formula:
uint32_t offset = b[0] + b[1] + b[2] + b[3];
offset = offset % 728;
offset = offset + 12;

E: HMACsha256 over entire 1536 bytes except zone E (the digest itself) using fisrt 30 bytes from genuineFPKey as key

I: the client's public key from the DH key pair

L: The location of the client's public key computed with this formula:
uint32_t offset = b[0] + b[1] + b[2] + b[3];
offset = offset % 632;
offset = offset + 772;

Of course, DH key must be computed before computing zone E

Credits:
Gavriloaie Eugen-Andrei (shiretu@gmail.com)(http://www.rtmpd.com/)
Luke Kenneth Casson Leighton (lkcl@lkcl.net)(http://lkcl.net/)

Server response (3072 bytes)

Start	Stop	length	Semnification	Zone name
0	3	4	uptime	A
4	7	4	version	B
8	11	4	digest offset	C
12	12+digest offset-1	digest offset	Unknown zone	D
12+digest offset	12+digest offset+31	32	digest	E
12+digest offset+32	739	696-digest offset	Unknown zone	F
740	771	32	Unknown zone	G
772	772+dh offset -1	dh offset	Unknown zone	H
772+dh offset	772+dh offset+127	128	dh	I
772+dh offset+128	1403	504-dh offset	Unknown zone	J
1404	1531	128	Unknown zone	K
1532	1535	4	dh offset	L
1536	3039	1504	Unknown zone	M
3040	3071	32	2 stage Hash	N

A: I always put it 0

B: Impersonate with 3.5.1.1 (4 bytes: 3,5,1,1)

C: the bytes in this zone gives the offset to the digest with the formula:
uint32_t offset = b[0] + b[1] + b[2] + b[3];
offset = offset % 728;
offset = offset + 12;

E: HMACsha256 over first 1536 bytes except zone E (the digest itself) using fisrt 36 bytes from genuineFMSKey as key

I: the server's public key from the DH key pair

L: The location of the server's public key computed with this formula:
uint32_t offset = b[0] + b[1] + b[2] + b[3];
offset = offset % 632;
offset = offset + 772;

Of course, DH key must be computed before computing zone E

N: 2 stage sha256 hash
chalange=hmacsha256 over zone E from client chunk 1 using entire genuineFMSKey as key
final hash=hmacsha256 over zone M using chalange as key

Credits:
Gavriloaie Eugen-Andrei (shiretu@gmail.com)(http://www.rtmpd.com/)
Luke Kenneth Casson Leighton (lkcl@lkcl.net)(http://lkcl.net/)

Client chunk 2 (last 1536 bytes)

Start	Stop	length	Semnificatio	Zone name
0	1503	1504	Unknown zone	A
1504	1535	32	2 stage Hash	B

B: 2 stage sha256 hash
chalange=hmacsha256 over zone E from server using entire genuineFPKey as key
final hash=hmacsha256 over zone A using chalange as key